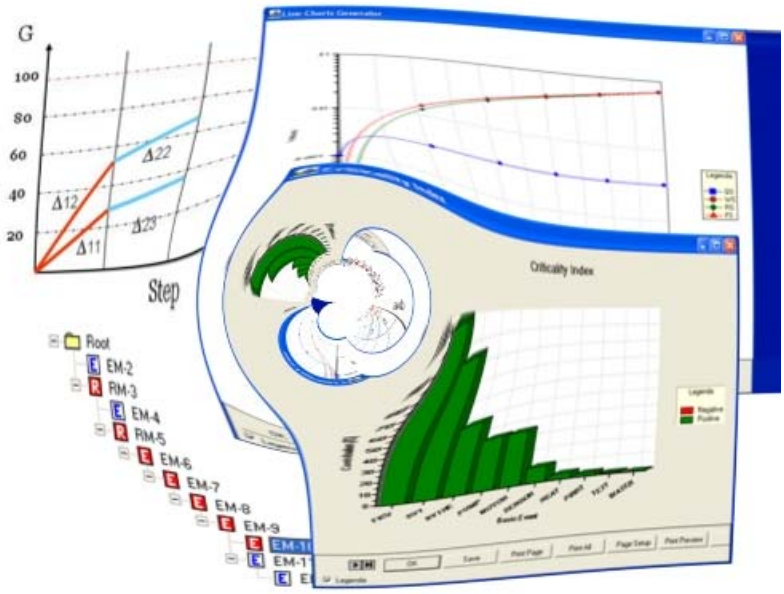
JRC Scientific and Technical Reports

Concurrent Importance and Sensitivity Analysis applied to multiple Fault Trees

Combination of Importance and Sensitivity Analysis to improve the design of critical systems or to prove that the design satisfies the pre-defined goals

Sergio Contini, Luciano Fabbri and Vaidas Matuzas



EUR 23825 EN - 2009

JRC EUROPEAN COMMISSION

ipsc Institute for the Protection and Security of the Citizen

The mission of the Institute for the Protection and Security of the Citizen is to provide research results and to support EU policy-makers in their effort towards global security and towards protection of European citizens from accidents, deliberate attacks, fraud and illegal actions against EU policies

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Address: L. Fabbri, EC JRC Ispra, Ispra (VA) Italy
E-mail: luciano.fabbri@jrc.ec.europa.eu
Tel.: +39.0332.78.5801
Fax: +39.0332.78.9007

http://ipsc.jrc.ec.europa.eu/
http://www.jrc.ec.europa.eu/

JRC51432

EUR 23825 EN

ISSN 1018-5593

Luxembourg: Office for Official Publications of the European Communities

Printed in Italy

EXECUTIVE SUMMARY

Complex systems are usually characterised by a set of potential failure states (i.e. Top-events), which are strictly associated with accident scenarios with unacceptable consequences. The study of the system failure states via Fault-tree Analysis allows determining the accident scenarios' occurrence probability and the importance measures of components' failure modes.

The use of Importance and Sensitivity Analysis (ISA) combined with the results of Fault-tree Analysis constitutes a very powerful tool to improve the design of critical systems or to prove that the design satisfies the general or specific requirements. Importance and Sensitivity Analysis is normally addressed to envisage the output behaviour of a model as a consequence of the variation of the input variables, with the purpose of identifying input variables that are more significant in term to their contribution to the model output. Referring to Fault-trees, the model's output under interest is the likelihood of occurrence of the associated Top-events. The input variables are all possible failure modes of the system's components, which, in the Fault-tree theory, are indicated as primary or basic events. The identification of the weakest part (components) in the system in term of their contribution to risk, and in turn the identification of those elements that require further design improvement, is the final objective of such an analysis. This is conducted by defining proper importance measure for each component, which describe its level of criticality for the specific Top-event of interest.

Complex systems are normally characterised by a number of potential accident scenarios and their related Top-events. In general, the different Fault-trees describing the different Top-events might contain common basic events. Current approaches to Importance and Sensitivity Analysis are based on the Sequential analysis of the different Fault-trees i.e. given N Fault-trees they are independently analysed one after another. It results that any proposal for the modification of a certain system's component, which results from the analysis of a certain Top-event, has to be reassessed when performing the analysis of other Fault-trees containing the same component. This reiteration process makes the overall analysis.

The present report presents a different approach to Importance and Sensitivity analysis, which is based on the Concurrent Analysis of all Fault-trees of the system. The Concurrent Analysis was already implemented in the past [1]; it was based on the definition of global importance indexes for all basic events that were shared by two or more Fault-trees. Although it was applied with success to a real system, that method was characterised by a number of limitations. The approach here proposed overcomes the drawbacks of the previous implementation and it introduces a selective method to reduce the occurrence probability of each Top-event. In particular, different probabilistic goals are selected for different Top-events, depending on their specific contribution to risk. Another innovative aspect of the proposed approach is that the method is extended also to identify "over-reliable" system functions (if any) on which the reliability/maintainability characteristics of the involved components can be relaxed with consequent cost saving. The overall result of the analysis is a uniformly protected system satisfying the predefined probabilistic goals. In order to implement the novel approach to Importance and Sensitivity Analysis a dedicated software tool was developed (CISA) which makes use of the JRC-ASTRA software for Fault-tree analysis. The present report describes the methodology, summarises the main features of the CISA software and provides an example of application.

TABLE OF CONTENTS

1. INTRODUCTION

Any system may present different potentially dangerous failure states, commonly indicated as *Top-events*, which are directly associated with accident scenarios. These failure states are commonly identified through the application of systematic methodologies, such as for instance HAZOP, FMEA, and may have different importance with reference to their potential consequences on the plant integrity, and in turn on the population and the environment. The study of the system failure states, i.e. of the occurrence probability/frequency of the accident scenarios can be performed by means of various system analysis techniques. The most popular one among practitioners is the Fault-tree Analysis (FTA). Specifically, Fault-trees allow describing systematically the cause-effect relationships amongst failure events from system to component, at different levels of detail. In particular, FTA allows studying the role played by the different failure modes associated with the system's components (hereafter referred to as *basic events: BE*), which might have a different impact on the occurrence probability of Top-events. The Fault-tree technique presents the important advantage of being applicable to systems containing any number of components. In addition, Fault-tree construction procedure is very systematic. The limitation relates to the use of components' binary models, which means that each component is represented only by two possible states: working and failed. In addition, the quantification requires that all components be independent, i.e. the state of any component must not influence (or must not be influenced by) the state of all other components.

The quantification of the Fault-tree allows determining the reliability parameters of interest for design improvement. In particular, this analysis provides the so-called Minimal Cut Sets, MCS (i.e. the minimum sets of components whose failure lead to system failure), their occurrence probability and the system failure probability P_{top}. If the failure probability P_{top} is considered as not-acceptable, a design review has to be made with the specific objective of reducing P_{top} to an acceptable predefined value P_G.

Given the situation in which the occurrence probability of a Top-event is not-acceptable (i.e. $P_{top} > P_G$), it is necessary to answer to the following questions:

- How can the system be improved?
- On which basis a better design solution can be identified?
- How is it possible to make the system uniformly protected against accidents, i.e. how can we get rid of its weakest parts?
- Are there functions over protected or over reliable? How can we eliminate them?
- What about if more design alternatives could be adopted?

A possible way forward to address these questions is the use of Importance and Sensitivity Analysis (ISA) combined with the results of FTA. This consists of a methodology to study the output behaviour of a model following the variation of input variables with the final objective of identifying those variables that give the most significant contribution. For Fault-trees, the model's output is the Top-event probability whilst the input variables are the components' failure modes, usually referred to as *primary or basic events (BE)*[1].

The introduction of *importance measures (or indexes)* for basic events, allows the analyst to derive information about the relative risk-significance of the associated components with respect to other components in the system. Each index is a measure of the importance of the contribution of a certain BE on the occurrence probability of the Top-event. The most sensitive failure modes (basic events),

[1] For the purposes of this report we will generally refer to component failure or basic event without distinction, due to the use of a binary model, i.e. the failure of a component is represented in the model by the verification of the associated basic event.

which are associated with the most critical components, are those having highest importance indexes, giving the maximum reduction of the Top-event probability for a given reduction of the associated BE probability. These BEs are clearly associated with the system function that needs to be improved. Once the most "sensitive" failure modes are identified, some system improvements can be made by modifying the design of the associated components. More specifically, a critical component can be substituted either with another component of better quality and/or better maintainability and/or better testing strategy, or with a subsystem where the component has a redundant part, as e.g. parallel, stand-by, K out of N, and so on. A point to note is that generally speaking, the design modifications which are practically implemented are those involving the system's components of safety functions, which require lower/negligible costs if compared with production/process related components.

Importance measures can normally be classified into two broad categories: structural and probabilistic. The importance measures belonging to the structural category depend exclusively on the location of the associated component within the system. They depend therefore, on the Top-event's structure function (i.e. the way the BE combines within the MCS). By contrast, the importance measures of the second category are those also associated with the reliability properties of the related components, i.e. their probability of failure.

Complex systems are usually characterised by a number of potential failure states (Top-events). Each different Top-event is associated with accident outcomes, which are characterized by different level of consequences. For each of these potential accident scenarios, a Fault-tree is constructed. Hence the resulting N Fault-trees can be analyzed independently, one at the time, starting for instance from those having most severe consequences or higher estimated risk. This approach is indicated as **Sequential Importance and Sensitivity Analysis** (**SISA**). The main complication which characterises this approach arises from the fact that -especially for complex systems- the N Fault-trees describing the different Top-events might contain common basic events. It results that any proposal for a modification of the system resulting from the analysis of the *k*-th Fault-tree would require the analysis' update of all the Fault-trees previously analyzed (i.e. from 1 to *k*-1). In summary, the sequential analysis presents some clear practical disadvantages. Firstly, the analyst cannot fully realize the actual impact on the overall system safety from a modification that results from the outcome of the sensitivity study conducted on a single Fault-tree at a time. Secondly, it may happen that the result of the sensitivity analysis requires some deeper modification (e.g. the use of redundancies), implying a modification of several Fault-trees. Thirdly, the cost of the overall analysis might be significant because of repetitions, reiterations and overlapping. As a matter of fact, any system modification resulting from the analysis of any Fault-tree would require updating and re-analysing all previously-analysed Fault-trees, which contain the modified components. These limitations are amplified when considering problems with conflicting requirements, as for instance safety and production loss. Indeed, the reduction of the failure probability of Top-events is generally achieved through the improvement of the safety/control functions which, due to the extensive use of fail-safe components, would lead to a decrease of the system availability. A better trade-off between these two conflicting situations would be a concurrent analysis on all Fault-trees describing the system, in which both unavailability and safety functions are taken into account.

Indeed, a possible way forward to overcome the limitations of the SISA approach is to perform the Sensitivity Analysis on all Fault-trees concurrently. This approach has been called **Concurrent Importance and Sensitivity Analysis** (**CISA**), which was implemented in the past as an add-on module of the ASTRA tool-set [2] and successfully implemented in a practical case [3].

The present report introduces a further improvement of the CISA methodology. In particular the main bottleneck of the previous formulation of CISA was the necessity to use different subjective weighting factors for the different Top-events, to account for the severity of the associated scenarios. The newly

proposed approach offers the advantage of removing this subjective weighting factor in the calculation of components' *global importance index*.
In addition, the method addresses also components with lowest importance indexes, which may be associated with "over-reliable" or "over-protected" functions in the system. This with the final objective of uniformly protecting the system, i.e. avoiding not only "weak functions", causes of system failure, but also uselessly "over-reliable functions", causes of major costs. Hence, the additional cost for reducing the occurrence frequency of certain Top-events could be partially compensated by relaxing the reliability/maintainability characteristics of those functions that are over protected.

This report is structured into the following sections. Section 2 covers overall aspects concerning importance and sensitivity analysis. Section 3 presents the Concurrent Importance and Sensitivity analysis and addresses the extension of the methodology to the case of N Fault-trees. Section 4 briefly describes the main features of software CISA to implement the methodology. Section 5 provides an application example and the practical comparison of sequential and concurrent analysis. Finally the appendix provides the list of equations that can be applied for determining the unavailability of redundant configurations, implemented in CISA as an external library. This library can be increased in the future according to the users' needs.

2. IMPORTANCE AND SENSITIVITY ANALYSIS (ISA)

2.1 Basic considerations

Methodologies such as FMEA and HAZOP are commonly applied to identify the accident scenarios i.e. potential adversary events leading to accidents or production loss. Accident scenarios can be described in terms of their possible causes via Fault-trees, in which the cause-effect relationships at a component and system level are analysed. Each accident scenario is therefore associated with a Top-event, for which the occurrence probability can be calculated using FTA.
The overall risk associated with the failure of a system is given by a set of triplets [4]:

$R = < S_i \;\; P_i \;\; C_i >$ $\qquad$ i=1,2,….

where S_i is a possible accident scenario for the system (Top-event), P_i is its occurrence probability, and C_i is the consequence in case of accident scenario's occurrence. The overall risk of the system can be represented on a log-log scale as depicted in Figure 1 where, for each accident scenario (squared-points), the values of its corresponding probability and consequence are given. Normally, three main zones are defined, which are divided by two straight lines representing the risk acceptance criteria. The area above the bold straight line is considered as the area in which the risk is unacceptable, whilst the area below the dotted line is where the risk is considered acceptable. The intermediate area is the ALARP region (As Low As Reasonably Practicable) in which efforts must be done to possibly reduce the risk by further decreasing the failure frequency and/or reducing the consequences to an extent that is practically feasible. The task of the system designer is to "move" the risk points towards the acceptable risk area through the improvement of the system safety and/or the mitigation measures.

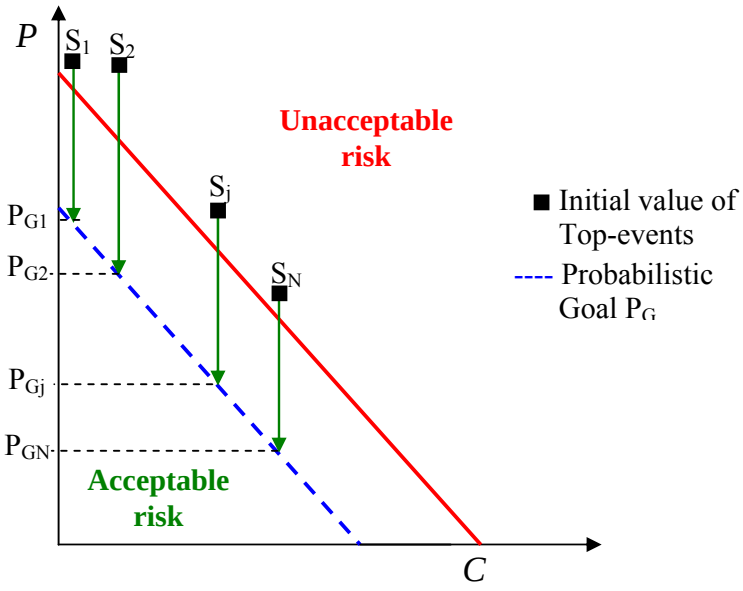


Figure 1 : Example of a Probability-Consequence plot showing unacceptable Top-events

In the present report, the problem of reducing the risk by reducing the accident occurrence probability is addressed. The activity on consequence reduction, which involves the introduction of mitigation measures, is outside the scope of the present work. In order to reduce the scenarios' probability, so as to shift down the corresponding risk point (see arrows in the figure), it is necessary to introduce structural modifications in the production/control system and/or to improve the protection system

functions. Normally, the second option is preferred for safety-related purposes, as the first is strictly linked to the production process and therefore any structural modification would impose a modification within the production line. In other words design modifications of the safety related functions are generally much less expensive than modifications of the production/control functions.

When risk reduction is deemed necessary, a specific goal has to be defined for each Top-event. Consequently, the probability of occurrence of the associated Top-event has to be reduced through the necessary design changes. In Figure 1 the vertical arrows represents the probabilistic reduction that is needed in order to render the risk acceptable. This reduction can be obtained by restraining the primary causes that can lead to the Top-event (basic events). The most effective approach is to operate on those basic events which contribute most to the probability of occurrence of the Top-event (i.e. those having highest importance indexes).

Before describing the general aspects of the Importance and Sensitivity analysis methodology it is worth to recall the main importance measures of basic events.

2.2 Importance Measures in Fault-tree Analysis

Importance measures of basic events are strictly associated with the risk-significance of the related components. In particular, they are normally used to rank the system's components with respect to their contribution to the reliability and availability of the overall system. Thus they provide an important indication about the components to be improved in order to increase the reliability and the availability of the associated system.

Importance Measures (also referred to as Importance Indexes) can normally be classified into two general categories: structural and probabilistic. Importance measures belonging to the former category depend exclusively on the location of the component in the failure logical functions of the system, which is described as the disjunction of MCS; indeed, an event appearing in MCS of order 1 is structurally more important than an event appearing in MCS of order 2, and so on. In the second category, the importance measures are also related to the failure probability of the associated component.

The importance measures that are considered in this report are applicable to coherent systems, in which Top-events are represented by AND-OR operators, i.e. logical functions that do not contain negated variables.

2.2.1 Definition of coherent systems

Let $\Phi(\mathbf{x})$ be a binary function of a vector of binary variables $\mathbf{x} = [x_1, x_2, \dots, x_n]$, representing the failure states of the *n* system's components. $\Phi(\mathbf{x})$ represents the logical function of the Top-event describing one of the system failure states. Assume a failure representation: $x_i = 1$ represents the failure of component *i*, and $\Phi(\mathbf{x}) = 1$ the system failure for the Top-event under consideration.
Analogously, $x_i = 0$ (component working) and $\Phi(\mathbf{x}) = 0$, (system working).

A binary structure function $\Phi(\mathbf{x})$ is said to be coherent if the following conditions hold:

a) $\Phi(\mathbf{x})$ is monotonic (non decreasing) in each variable, i.e. $\Phi(\mathbf{x}) \geq \Phi(\mathbf{y})$ if $\mathbf{x} > \mathbf{y}$, where **x, y** are two state vectors of $\Phi(\mathbf{x})$; $\mathbf{x} > \mathbf{y}$ means that $x_i \geq y_i$ for every i and $x_i > y_i$ for some i.

b) Each x_i is relevant, i.e. $\Phi(1_i, \mathbf{x}) \neq \Phi(0_i, \mathbf{x})$ for some vector **x**, where:

$\Phi(1_i, \mathbf{x}) = \Phi(x_1, x_2, .. , x_{i-1}, 1, x_{i+1},..., x_n)$
$\Phi(0_i, \mathbf{x}) = \Phi(x_1, x_2, ... , x_{i-1}, 0, x_{i+1},..., x_n)$.

In practical terms this means that:

- the status of the system with *k* components failed cannot be better then the status of the system with a greater number of failed components;

- there are no components whose status is always indifferent for the system state represented by the structure function $\Phi(\mathbf{x})$.

Note that $\Phi(1_i, \mathbf{x}) \geq \Phi(0_i, \mathbf{x})$ means $\Phi(1_i, \mathbf{x}) = \Phi(0_i, \mathbf{x})$ or $\Phi(1_i, \mathbf{x}) > \Phi(0_i, \mathbf{x})$, which is equivalent to say that $\Phi(1_i, \mathbf{x})\ \Phi(0_i, \mathbf{x}) = \Phi(0_i, \mathbf{x})$. Moreover, $\Phi(\mathbf{1}) = 1$, i.e. if all components are failed the system is failed, and $\Phi(\mathbf{0}) = 0$, i.e. if all components are working the system is working, where: $\mathbf{1} = [x_1=1, x_2=1, \dots, x_n=1]$ and $\mathbf{0} = [x_1=0, x_2=0, \dots, x_n=0]$.

2.2.2 Importance measures in coherent systems

Importance measures of basic events have assumed a very important role in system reliability which is testified by the very rich literature, see e.g. [5]. The following probabilistic importance measures are currently in use for risk assessment purposes:

- Birnbaum measure
- Criticality importance
- Risk Achievement Worth
- Risk Reduction Worth
- Fussell-Vesely importance
- Differential importance measure

Birnbaum importance index, IB

One of the basic parameters is the probability that the component is critical. A variable x_k, associated with e.g. the failed state of the component *k* is critical for the Top-event if the Top-event state takes the same value of the component state, i.e. if the component is working ($x_k = 0$) then Top = 0; if the component takes the failed state ($x_k = 1$) then Top = 1. Hence, each event of the Fault-tree can be associated with a Boolean function describing the conditions for the occurrence of its critical state.

Let $\Phi(\mathbf{x})$ be the Boolean function of a Fault-tree, where $\mathbf{x} = (x_1, x_2, \dots, x_n)$ is the vector of binary variables associated with the basic events. It is well know that:

$$\Phi(\mathbf{x}) = x_k\, \Phi(1_k, \mathbf{x}) + (1 - x_k)\, \Phi(0_k, \mathbf{x}) \qquad (2.1)$$

Accordingly the variable x_k is critical if:

$x_k = 1$ implies $\Phi(\mathbf{x}) = \Phi(1_k, \mathbf{x}) = 1$; and

$x_k = 0$ implies $\Phi(\mathbf{x}) = \Phi(0_k, \mathbf{x}) = 0$, i.e. $\overline{\Phi(0_k, \mathbf{x})} = 1$

Hence, the logical function describing the critical state for a generic variable x_k is expressed as:

$$\Phi(1_k, \mathbf{x}) \wedge \overline{\Phi(0_k, \mathbf{x})}$$

The probability that such a function occurs is given by:

$$\Pr[\Phi(1_k,\mathbf{x}) \wedge \overline{\Phi(0_k,\mathbf{x})} = 1,t] = \Pr[\Phi(1_k,\mathbf{x}) = 1,t] - \Pr[\Phi(1_k,\mathbf{x}) \wedge \Phi(0_k,\mathbf{x}) = 1,t]^2 \quad (2.2)$$

In the above equation t ($0 < t \leq T$), where T is the mission time, indicates the dependence on time of the failure probability.
If the generic variable x_k belongs to a coherent Fault-tree, then:

$$\Pr[\Phi(1_k,\mathbf{x}) \wedge \Phi(0_k,\mathbf{x}) = 1,t] = \Pr[\Phi(0_k,\mathbf{x}) = 1,t].$$

Therefore:

$$\Pr[\Phi(1_k,\mathbf{x}) \wedge \overline{\Phi(0_k,\mathbf{x})} = 1,t] = \Pr[\Phi(1_k,\mathbf{x}) = 1,t] - \Pr[\Phi(0_k,\mathbf{x}) = 1,t]$$

This probability is referred to as Birnbaum importance index, i.e.:
$IB_k(t) = \Pr[\Phi(1_k,x) = 1,t] - \Pr[\Phi(0_k,x) = 1,t]$

For the sake of clarity, the following simpler notation will be used throughout the report. The dependence on time will be omitted, meaning that the equations are applicable to any time t ($0 < t \leq T$).

$$Q = \Pr[\Phi(\mathbf{x}) = 1,t]$$

$$Q_{1k} = \Pr[\Phi(1_k,x) = 1,t]$$

$$Q_{0k} = \Pr[\Phi(0_k,x) = 1,t]$$

$$q_k = \Pr[x_k = 1,t]$$

Using the new notation the Birnbaum importance index can be written as:

$$IB_k = Q_{1k} - Q_{0k}$$

From eq. (2.1) passing to probabilities one gets:

$$Q = q_k\, Q_{1k} + (1 - q_k)\, Q_{0k} \quad (2.3)$$

Hence it is straightforward to see that:

$$IB_k = \frac{\partial Q}{\partial q_k}$$

Criticality index, IC_k

This index represents the probability that the event x_k is critical and its occurrence leads to system failure. In other words, given the system in the failed state, the Criticality index of x_k is the probability that x_k occurred last. In this context it is easy to show that:

$$IC_k = IB_k \frac{q_k}{Q} \quad (2.4)$$

[2] Equation (2.2) can be justified as follows. Given two independent events A, B it is possible to write A = A (B + $\bar{B}$). Hence, A = A B + A $\bar{B}$. Being A B and A $\bar{B}$ mutually exclusive events then, passing to probability,
Pr(A) = Pr(A B) + Pr(A $\bar{B}$) from which Pr(A $\bar{B}$) = Pr(A) - Pr(A B)

From eq. (2.4) it results that the criticality index can be written as:

$$IC_k = IB_k \frac{q_k}{Q} = \frac{\partial Q}{\partial q_k}\frac{q_k}{Q} \tag{2.5}$$

And, therefore, it can be interpreted as the relative variation of the Top-event occurrence probability vs the relative variation of the occurrence probability of the k-th basic event.

Risk Achievement Worth, RAW_k

The RAW is defined as a measure of the change of the system failure probability when x_k is supposed failed or removed e.g. for test/maintenance operations. In calculating the RAW it is important to consider all other components that are dependent by the failure/removal of x. According to the definition:

$$RAW_k = \frac{Q_{1k}}{Q} \tag{2.6}$$

Risk Reduction Worth RRW_k

The RRW is defined as a measure of the change of the system failure probability when x_k is supposed to be perfectly working:

$$RRW_k = \frac{Q}{Q_{0k}} \tag{2.7}$$

Clearly RAW and RRW are strictly related. Indeed given: $\Phi(\mathbf{x}) = x \wedge \Phi(1_k, \mathbf{x}) + \bar{x}\,\Phi(0_k, \mathbf{x})$

and passing to probabilities:

$$Q = q_k\, Q_{1k} + (1 - q_k)\, Q_{0k} \tag{2.8}$$

Dividing both members by Q and after a little algebra the following relationship can be obtained:

$$RAW_k = \frac{1}{q_k}\left(1 - \frac{1 - q_k}{RRW_k}\right) \tag{2.9}$$

Moreover the RRW is related to IC. Indeed (2.8) can be re-written as:

$$Q = q_k \{Q_{1k} - Q_{0k}\} + Q_{0k}$$

Dividing by Q and after a little algebra the following relationship can be obtained:

$$1 = \frac{q_k\, IB_k}{Q} + \frac{1}{RRW_k} \quad \Rightarrow \quad RRW_k = \frac{1}{1 - IC_k} \tag{2.10}$$

Fussell-Vesely

This importance index, also referred to as "fractional contribution" is a measure of the contribution of x_k to the Top-event occurrence without being critical. The variable x_k contributes to system failure when a minimal cut set (MCS) containing such a variable occurs. Hence the Fessell-Vesely index is expressed as:

$$FV_k = \frac{\Pr[\bigcup_s C_s = 1]}{Q} \cong \frac{Q - Q_{0k}}{Q}$$

where C_s is the s-th Minimal Cut Set containing x_k.

It is easy to verify that the FV index is related to the RRW by:

$$FV_k \cong 1 - \frac{1}{RRW_k} \quad \Rightarrow \quad RRW_k \cong \frac{1}{1 - FV_k} \tag{2.11}$$

Hence, from (2.9) it follows that $FV_k \cong IC_k$ if the rare event approximation holds. More precisely $FV_k > IC_k$

Differential Importance measure **$\mathbf{DIM_k}$**

The DIM importance measure of a basic event x_k gives the fraction of the total variation of Q due to a small variation of the probability of x_k. According to the general definition, the Differential Importance Measure (DIM) of the *k*-th component/basic event is given by [6]:

$$DIM_k = \frac{\frac{\partial Q}{\partial q_k} dq_k}{\sum_{i \in x} \frac{\partial Q}{\partial q_i} dq_i}$$

which represents the fraction of the variation in Q due to a change in variable x_k and normalised to the sum of the variation of the same parameter due to the change in all other variables. The main advantage of DIM is that it is characterised by the additivity property, i.e. the joint DIM of a set of basic events is the sum of individual DIMs. In addition, the sum of the DIMs of all basic events (for each Fault-tree) equals unity. Finally, DIM is strictly related to the Birnbaum and the Criticality indexes. Indeed, by assuming uniform changes in the variables:

$$dq_i = dq_k \quad \forall\, i,k \in \{\mathbf{x}\}$$

the corresponding expression of DIM (hereafter indicated with the H1 suffix) becomes:

$$DIM_k^{H1} = \frac{\frac{\partial Q}{\partial q_k}}{\sum_{i \in x} \frac{\partial Q}{\partial q_i}} = \frac{IB_k}{\sum_{i \in x} IB_i} \tag{2.12}$$

whilst by assuming proportional changes in the parameters i.e.:

$$\frac{dq_k}{q_k} = \frac{dq_j}{q_j} \quad \forall i,k \in \{\mathbf{x}\}$$

the corresponding expression of DIM (hereafter indicated with the H2 suffix) becomes:

$$DIM_k^{H1} = \frac{\frac{\partial Q}{\partial q_k} q_k}{\sum_{i \in x} \frac{\partial Q}{\partial q_i} q_i} = \frac{IC_k}{\sum_{i \in x} IC_i} \tag{2.13}$$

The sensitivity analysis method proposed within CISA can be applied by using any of the above listed importance measures, depending on the specific problem under study. However, and especially in the chemical sector, it is common to use the Birnbaum and Criticality indexes or the Fussel-Vesely index.

Table 1 provides some information on how to use the former indexes in a combined way.

For sensitivity analysis purposes it is easy to see that, given the IB and IC indexes, the most important components are those with both indexes high (4), followed by those with IB low and IC high (3).

If the FV index is considered, there is no possibility to discriminate between cases (2) and (3).

		IB	
		LOW	**HIGH**
IC	**LOW**	**The situation is not critical, i.e. the involved component need not to be improved** 1	**The component is in MCS of low order or that it is combined with components of high probability; however the component is reliable, which means that it is the structure function that needs to be improved, not the component** 2
	HIGH	**The probability that the component is critical is very low, whereas the failure occurrence probability of the associated event is high, which means that it could be useful to select the component for design improvement** 3	**The component is definitely a weak element for the system** 4

Table 1: Birnbaum vs. Criticality Index

2.3 Importance and Sensitivity Analysis: General aspects

The Importance and Sensitivity Analysis (ISA) is a consolidated procedure applied during the system's design phase to identify the weakest parts of the system, i.e. those components whose failure modes (represented as basic events in FTA) give the greatest contribution to the likelihood of occurrence of the most relevant Top-events. A point to note is that the overall analysis is not very much important to assess the absolute value of the Top-event occurrence probability, but to get reference parameters to identify those critical basic events in terms of their contribution to risk. Once the components are identified, suitable design modifications can be considered in order to reduce the system failure probability. The general procedure to apply ISA is mainly based on three steps:

Step 1: Identification of critical components Ranking of the different system's components' failure modes according to their importance to system failure (importance measures). In particular, the use of importance measures for each basic event, allows getting information on the relative risk-significance of the associated components with respect to other components in the system. Each index measures the importance of the failure of a BE on the occurrence probability of the Top-event.
Step 2: Design Alternatives Having identified the weakest parts of the system (i.e. those components having highest importance measures), the design can be improved by adopting one or more design strategies (i.e "*design alternatives*"). These mainly consist of replacing the selected components with others of better quality or by applying the redundancy concept or by deeply modifying the system failure logic.
Step 3: Re-assessment & Design Solution Following the design modification the Fault-tree is updated and re-analysed to assess the effects of the improvement made, that is the impact of the adopted design alternatives to the system failure probability and the selection of the most convenient alternative by taking into account the existing constraints (e.g. cost, space, and weight). Clearly, the selected design modification will require some investments, which could be more or less significant.

These three steps are iteratively applied until the pre-defined goals are achieved.

The ISA process outlined above is conducted on all Fault-trees describing all possible failures of the associated system. Generally practitioners analyse Fault-trees sequentially, starting from those having more severe consequences. If two or more fault trees are associated with the same level of consequences the choice of the fault tree from which to start the analysis is generally random and based on subjective considerations. In the present report, this approach is referred to as "**Sequential ISA**" (**SISA**). Figure 2 gives a schematic diagram of SISA for a system with N=3 Fault-trees.

For each Top-event, let $Q^{(0)}$ be the value of its occurrence probability before starting the Sensitivity Analysis procedure (initial condition). Let P_G be the assigned goal to be achieved. The comparison of $Q^{(0)}$ and P_G gives the designer an indication about the effort needed to improve the system. Obviously, if $Q^{(0)} \leq P_G$ no further improvement is needed. By contrast, when $Q^{(0)} > P_G$, the goal P_G can be reached after one or more improvement steps which are associated with system modifications. The Top-event probability Q, changes from $Q^{(0)}$ at step 0 to $Q^{(i)} < Q^{(i-1)}$ at the *i*-th step.

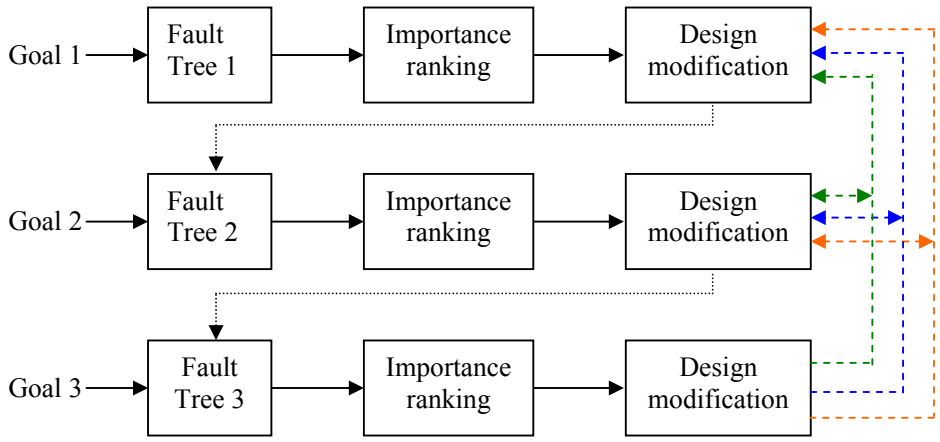


Figure 2: Schematic diagram of the Sequential Importance and Sensitivity Analysis (SISA)

At the generic *i*-th step of the ISA process, the probabilistic quantification provides the Top-event occurrence probability $Q^{(i)}$ and the components importance measures at step i. Since these measures are determined on a single Fault-tree they are hereafter referred to as "**Local Importance Indexes**" (**LII**). In general, the component with maximum LII values are selected and considered for design improvement. If a potentially useful design modification is identified then the Fault-tree under consideration is analysed to verify whether to retain it or not. In the positive case, i.e. the modification is retained, if the next Fault-tree to be examined contains the modified components, then it is necessary to properly modify it before proceeding with its analysis. This is represented in Figure 2 with connections between "Design modification" and "Fault tree" blocks.

Moreover, a system modification following the analysis of e.g. the *j*-th Fault-tree should lead to the updating of all Fault-trees previously analysed (i.e. from 1 to *j*-1), which contain the modified component. This process is represented in Figure 2 by the arrows with dotted lines. In the current practice, this "backwards" re-analysis is not performed very often for two main reasons:

(i) the increase of the overall costs of the analysis, and

(ii) the coherency of the Fault-trees, which implies that a component modification that leads to a failure probability reduction of the *j*-th Top-event cannot increase the failure probability of the other Top-events.

It is evident that the Sequential ISA might lead to make some system functions more reliable than needed.

An important point to be considered is that by means of the SISA approach it is not possible to state that the identified design modification, which achieves the goal, is the most effective one, since it depends on the sequence of analysis of the fault trees. For example, in Figure 2 the sequence considered is FT1-FT2-FT3, but also other sequences could be considered, e.g. FT3-FT1-FT2, which might be more convenient, depending on the dependencies among fault trees. Unfortunately, it is not possible to know in advance which sequence is the best.
In practice the ISA approach is applied to one sequence only.

An alternative way of carrying out the sensitivity analysis is to perform it concurrently on the whole set of system's Fault-trees. This approach is hereafter referred to as "**Concurrent ISA" (CISA**). Figure 3 provides a schematic diagram of CISA for N=3 Fault-trees.

The substantial difference between SISA and CISA is the determination of the **Global Importance indexes (GII)** of basic events, i.e. indexes determined on the basis of LII calculated in all Fault-trees. The GII ranking coincides with the LII ranking if all Fault-trees are independent, i.e. if they do not share any basic event. If fault-trees are not independent then, for a generic event x_k, $GII_k > \max(LII_k)$. The component with the maximum GII value is selected and considered for design improvement. If a useful design modification is identified, then all fault-trees containing the selected component are accordingly modified and re-analysed. It is clear that the CISA approach is particularly suitable also to face problems of conflicting requirements (e.g. unavailability vs. safety; no-intervention on demand vs. spurious intervention for protective systems) and to find suitable trade-offs.

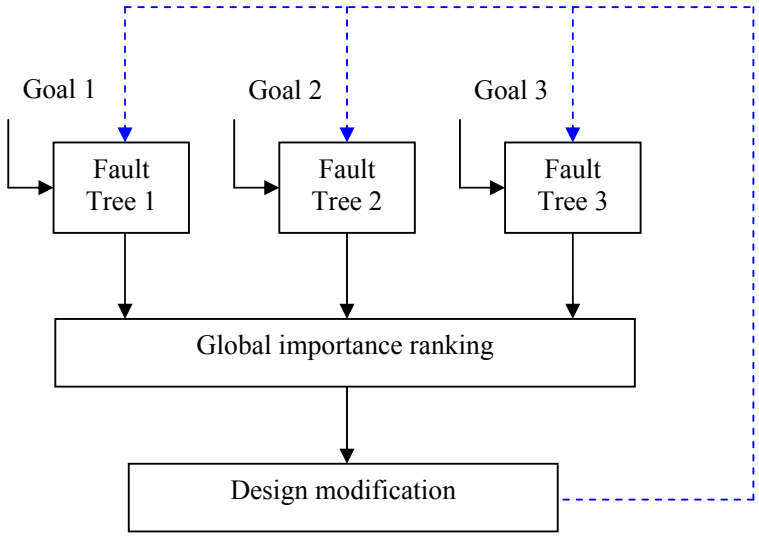


Figure 3: Schematic diagram of the Concurrent Importance and Sensitivity Analysis (CISA)

It is clear that the CISA approach does not present the problem of identifying the fault tree from which to start the analysis, since fault trees containing the basic event with the highest GII are concurrently analysed. Hence the best effective design modifications can always be identified, due to the selection of the weakest points of the system.

For both SISA and CISA, each Fault-tree has its own associated goal P_{Gi} (i=1,..,N) (see Figure 2 and Figure 3). This is typical of any ISA procedure, which aims at reducing the occurrence probability of each Top-event to the reference goal. This allows selecting the proper probabilistic reduction to be attained depending on the Top-event position in the risk curve (see Figure 1).

In summary the following scheme provides a general comparison of the SISA and CISA approaches for Fault-tree Importance and Sensitivity Analysis:

SISA and CISA are <u>equivalent</u> WHEN: - only one Fault-tree is involved in the analysis; - all Fault-trees are independent, i.e. if there are no common events
CISA is <u>superior</u> to SISA WHEN there are common events, since: - the designer can immediately see the impact on all Top-events of each adopted design modification; - the determination of components criticality, by means of GII, takes into account the probabilistic dependence between Top-events; - the identification of the best design modification does not depend on the fault tree sequence; - the cost of the analysis is always lower than the cost with SISA.

3. THE FORMULATION OF THE CISA METHOD

For the sake of clarity the description of the proposed CISA methodology will be given considering first its application to a single Fault-tree and then its extension to multiple Fault-trees, which represent the general case. The analysis method can be subdivided into two phases, referred to as:

- Goal achievement
- Cost reduction

The Goal Achievement Phase (GAP) aims at reducing the occurrence probability of the system's Top-events to an acceptable risk value.

The Cost Reduction Phase (CRP) aims at identifying the "over-reliable" functions through the determination of the least important components. As the weak points (from the reliability viewpoints) can be identified by means of the highest importance indexes, analogously the strongest points can be identified by means of the lowest importance indexes. In this way, the proposed method does not solely address the most critical components in terms of their contribution to risk, but it also focuses on those less critical components, which may be uselessly reliable.

3.1 Application of the methodology to a single Fault-tree

3.1.1 Goal Achievement Phase

The Goal Achievement Phase (GAP) aims at reducing the occurrence probability of the system's Top-events to an acceptable risk value (see Figure 1).

Let the occurrence probability be $Q^{(0)}(t)$ at mission time t[3], and $P_G < Q^{(0)}$ be the pre-assigned probabilistic goal to be achieved. The Goal Achievement Phase is specifically addressed to identify possible and effective design solutions which correspond to a reduction of the Top-event occurrence probability Q to such an extent that the goal is reached (i.e. $Q \le P_G$) also respecting existing constraints on e.g. cost, weight, and volume, as identified by the user.
Starting from $Q^{(0)}$ the goal P_G could be achieved in one or more steps, where at each step a system modification is adopted. The current Top-event probability Q changes from $Q^{(0)}$ at step 0 (initial condition) to $Q^{(1)} < Q^{(0)}$ as a consequence of the first design modification. At the generic *i*-th step, the difference between the Top-event failure probability $Q^{(i)}$ and the goal P_G is a measure of the effort needed to improve the system. The Total Gain percentage at the generic *i*-th step, indicated as $G^{(i)}$ and the percentage effort $E^{(i)}$ still to be done to reach the goal are given by:

$$G^{(i)} = \frac{Q^{(0)} - Q^{(i)}}{Q^{(0)} - P_G} 100\,; \qquad E^{(i)} = 100 - G^{(i)} \tag{3.1}$$

The goal is satisfied at step *i* when $Q^{(i)} \le P_G$, which means that $G^{(i)} \ge 100$.

All these quantities are graphically shown in Figure 4.

[3] reference to time will be hereafter omitted to simplify the notation

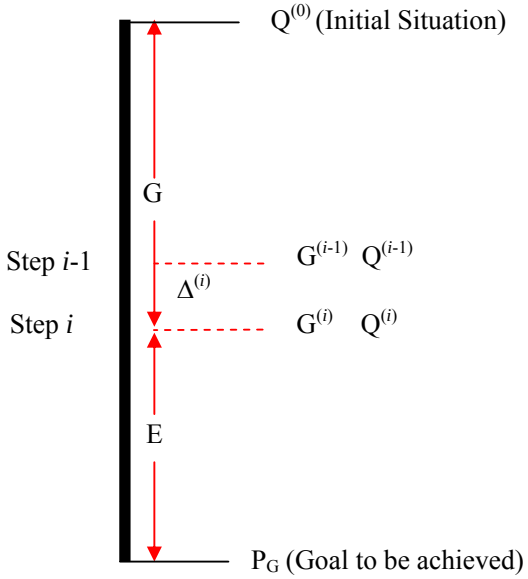


Figure 4 : Main parameters of the system improvement process at a generic step

The gain at the generic *i*-th step, with respect to the previous step (*i*-1) referred to as Step Gain percentage and represented as $\Delta^{(i)}$, is given by:

$$\Delta^{(i)} = \frac{Q^{(i-1)} - Q^{(i)}}{Q^{(0)} - P_G} 100 \qquad (3.2)$$

The component to consider at each step is the one having the highest importance index, i.e. the one with the highest contribution to the Top-event occurrence probability. Frequently the Criticality index IC_k is the selected importance index for such a purpose [1], since it is also a measure of the relative variation of the Top-event probability due to a given relative variation of the component failure probability. This statement can be justified as follows.

Let $\Phi(\mathbf{x})$ be the structure function of the Fault-tree under examination, where $\mathbf{x} = (x_1, x_2, ...x_n)$ is the vector of the Boolean variables (basic events). It is well known that, with respect to a given event x_k, the structure function Φ can be written as follows:

$$\Phi(\mathbf{x}) = x_k \; \Phi(1_k, \mathbf{x}) + \bar{x}_k \; \Phi(0_k, \mathbf{x})$$

Passing to probabilities:

$$Q = q_k \; IB_k + Q_{0k} \qquad (3.3)$$

By indicating with $q_k^{(i-1)}$ the failure probability of the *k*-th BE at the (*i*-1)-th step corresponding to the system failure probability $Q^{(i-1)}$, and with $q_k^{(i)}$ the value that corresponds to $Q^{(i)}$, from equation (3.3):

$$Q^{(i-1)} = q_k^{(i-1)} IB_k^{(i-1)} + Q_{0k}^{(i-1)}$$
$$Q^{(i)} = q_k^{(i)} \; IB_k^{(i-1)} + Q_{0k}^{(i-1)}$$

clearly the term $IB_k^{(i-1)}$ is the same in the above formulas because the Birnbaum of the k-th component does not depend on its unavailability but on those of the other components.

By assuming that $q^{(i)} < q^{(i-1)}$, which implies that $Q^{(i)} < Q^{(i-1)}$ (coherent system), and subtracting the second equation to the first one it results:

$$Q^{(i-1)} - Q^{(i)} = (q_k^{(i-1)} - q_k^{(i)})\, IB_k^{(i-1)}$$

which leads to:

$$\frac{Q^{(i-1)} - Q^{(i)}}{Q^{(i-1)}} = \frac{IB_k^{(i-1)} q_k^{(i-1)}}{Q^{(i-1)}} \frac{(q_k^{(i-1)} - q_k^{(i)})}{q_k^{(i-1)}}$$

Note that $IC_k^{(i-1)} = \frac{IB_k^{(i-1)} q_k^{(i-1)}}{Q^{(i-1)}}$ is the expression of the Criticality importance index of the k-th BE at the (i-1)-th step; after a little algebra, the following equation is obtained:

$$Q^{(i)} = Q^{(i-1)}[1 - IC_k^{(i-1)} \frac{(q_k^{(i-1)} - q_k^{(i)})}{q_k^{(i-1)}}] \qquad (3.4)$$

From equation (3.4) it results that $Q^{(i)}$ can be simply obtained by using the value of the system occurrence probability at the previous step without re-analysing the Fault-tree. This expression gives the new value of the Top-event occurrence probability at the i-th step of the ISA procedure, by operating on the k-th basic event only. The reduction in the failure probability of the selected component:

$$q_k^{(i)} < q_k^{(i-1)}$$

which is necessary to implement the ISA procedure, can be achieved in different ways, as e.g. by changing the intrinsic reliability/maintainability parameters of the involved component or by using redundant configurations. The first choice does not affect the structure of the system's Fault-trees containing this component and can be achieved though the following possible modifications:

- Reduction of the failure rate (i.e. by using a better quality component);
- Reduction of the mean-down-time (by improving the component maintenance);
- Modification of test intervals and/or of testing policy per tested component.

The second choice (redundant configuration) consists of replacing the involved component with two or more components of the same type connected in parallel or in stand-by. Possible configurations are e.g. parallel; stand-by, K/N of tested components with different testing policy (sequential / staggered).

It should be noted that the effect on the Top-event occurrence probability due to the use of any redundant configuration can rapidly be determined if there is no need to modify the Fault-tree. This is indeed the solution adopted in the software CISA described in Section 4: the redundant configurations are managed by a dedicated module implementing the equations provided in the Appendix. The fault-tree must be suitably modified only if the user realises the necessity to modify the system failure logic.

If the gain $G^{(i)}$ (eq. 3.1) corresponding to the chosen design modification is acceptable (i.e. $G^{(i)} \geq 100$), then the Fault-tree can be effectively updated and analysed (i.e. the i-th step is the last one), otherwise another modification has to be identified and tested in the same manner. Considerations on the existing constraints for the system under scrutiny (e.g. volume, weight, cost, etc) should clearly be taken into

account to further help identifying the best design alternative to be implemented. These constraints are considered by the user before adopting a design modification.

It should be noticed that at a given step of the ISA procedure, there might be different comparative alternatives to modify the *k*-th component under scrutiny, which would lead to a Gain increase. These alternatives can be managed by means of a decision tree, where each node has as many descendants as the number of identified potentially acceptable alternatives, as schematically shown in
Figure 5, where the root represents the initial design configuration.

At a given step each branch represents a modification of the reliability characteristics of the selected component. To each alternative a modification of the system design is associated. The acceptability of such a modification is clearly based on its impact on the reliability of the selected component but also on other considerations associated with the existing constraints.

This procedure leads to the development of a tree as represented in Figure 5. A path from the root to a terminal node represents a set of design modifications, which is a potentially acceptable solution for system design improvement. In other words a path is a set of design modifications compatible with all constraints. The Total Gain provides information on "How good" the *k*-th path is. In order to speed up the process, all alternatives at step *i* could be compared to continue only with those that seem to be the most promising, i.e. having comparatively higher Total Gain. Hence, potential alternatives recognised as less significant, can be removed to avoid developing branches that cannot lead to useful solutions.

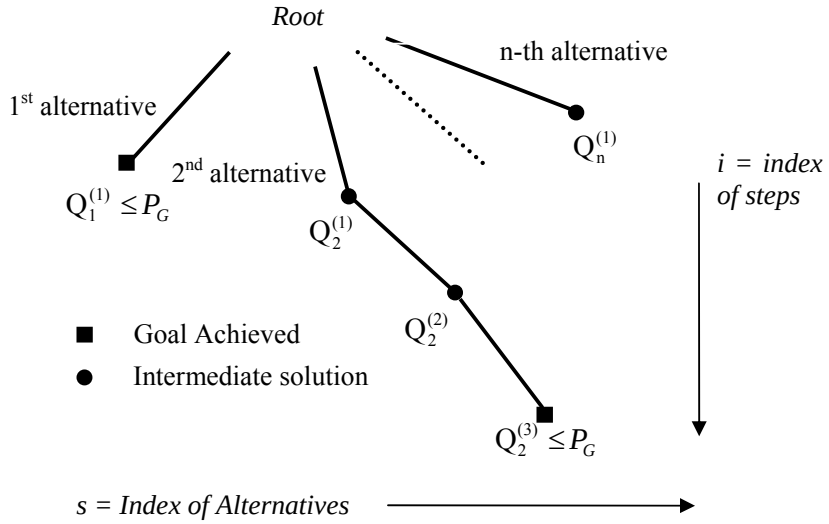


Figure 5: Schematic representation of different potentially acceptable alternatives (decision tree)

The decision tree depicted in
Figure 5 can also be referred to a group of components having comparable importance indexes, which are selected in the process for modification. In these cases the descendents refer to the possible different modification alternatives for this group of components. For each node of the branch, the failure probability of the overall system is illustrated on the figure. Specifically the subscript refers to the selected alternative whilst the superscript in brackets () refers to the step in the sequence of the same branch.

3.1.2 Cost Reduction Phase

Another innovative aspect of the method proposed in this report is the introduction of a Cost Reduction Phase (CRP). In this way, the proposed method does not solely address the most critical components in terms of their contribution to risk, but it also focuses on those less critical components, which are associated with uselessly reliable system functions. The identification of these components may

provide a contribution to costs reduction during the design phase, without affecting the achievement of pre-defined goals. In particular this phase aims at verifying whether the design configuration, resulting from the previous Gain Achievement Phase, may contain safety/control functions that present a failure probability which is unjustifiably low. The identification of these functions could allow reducing the cost of the final design solution by relaxing the reliability/maintainability characteristics of the involved components without compromising the achievement of the overall goal P_G. Hence the "cost" necessary for improving safety in GAP could be partially compensated by the solutions adopted in CRP. Ultimately the CISA methodology helps the user to produce / to prove that the system has no bottlenecks as well as no over-protected functions.

Contrary to the Goal Achievement Phase, the selection of the components to be examined for cost reduction is based on the minimum values of the importance indexes. A problem dealing with the determination of components with low importance index is associated with the fact that if the Fault-tree probabilistic analysis was based on the disjunction of MCS (i.e. the classical FTA approach), the determination of the criticality indexes would necessarily require the calculation of all MCS. As the number of MCS is often very high, the probabilistic analysis is often limited to the most important ones. By ignoring indeed the less significant MCS, it is evident that the contribution of components with low importance indexes is automatically neglected. This is probably the main reason why in practice the CRP phase was never proposed in the past.

By contrast, the introduction of the Binary Decision Diagrams (BDD) for Fault-tree calculations has allowed performing the exact quantification of Fault-trees without requiring the explicit determination of the MCS [7]. This method clearly facilitates a lot the identification and the determination of components having lower importance indexes and, in turn, the proper implementation of the Cost Reduction Phase. Hence, the CRP is applicable only if the fault tree analyser is based on the BDD approach.

Some strategies can be adopted for those components characterised by lower importance indexes. With reference to Table 1 these are e.g. those with low IB and low IC.
Depending on the type of component, the following decision can be taken:

- increase of failure rate (use a component of lower quality);
- increase of mean-down-time (allowing a longer repair time interval, delaying the repair activity, e.g. by avoiding to keep a spare part in the plant store);
- increase the time between tests (i.e. reduce the test frequency);
- change the testing policy (e.g. from staggered to sequential).

Thus, the component with the minimum Criticality index [5]can be examined to check whether a modification can be adopted by changing the component failure probability q_k with a higher value, which is still acceptable in terms of its impact on the system's failure probability (i.e. $Q^{(i)} \leq P_G$). This can be obtained re-writing equation 3.4 in which $q^{(i)} > q^{(i-1)}$, i.e.:

$$Q^{(i)} = Q^{(i-1)}\left[1 + IC_k^{(i-1)} \frac{(q_k^{(i)} - q_k^{(i-1)})}{q_k^{(i-1)}}\right] \qquad (3.5)$$

At step *i*-th of the modification process, if the estimated system's failure probability is not acceptable then another modification should be is examined. In summary, the following steps can be repeated as long as $Q \leq P_G$:

1. Select the component/event (x_k) having minimum IB, IC;
2. Identify the possible modification according to the type of component;
3. Determine the consequent variation of Q using equation (3.5);

4. If Q is acceptable the decision is then confirmed: the fault-tree is re-analysed and the new values are calculated, otherwise it is necessary to start back from step 1.

As for the previous case (GAP) a decision tree helps managing the possible design alternatives.

From a preliminary analysis, the effectiveness of the proposed method can by strongly influenced by the uncertainty associated with the Top-events' occurrence probability. As the method consists of comparing this value with prefixed probability goals, this aspect can have a significant impact on the final conclusions and the proposed design modifications. Clearly this aspect is of paramount importance and it represents one of the first topics for future investigation.

3.2 Extension of the methodology to multiple Fault-trees

3.2.1 Background

The CISA methodology is based on the determination of the Global Importance Indexes of basic events/components, which are calculated from all system's Fault-trees.
As previously mentioned, this method was already proposed in the past. However the approach had an inherent drawback as it required the use of subjective weighing factors to address the importance of each Fault-tree on the overall risk function.

The present report introduces a more objective and coherent approach to implement Importance and Sensitivity Analysis, which is based on the selective reduction of the occurrence probability of each Top-event. This is conducted in such a way to reduce the risk of the associated scenarios to an acceptable level. To achieve this objective, different probabilistic goals are selected for the different Top-events, depending on their specific contribution to risk i.e. depending on the position of the corresponding risk points on the risk-plot (i.e. *consequence* vs. *frequency*-graph, see Figure 1).

The two phases previously described with reference to a single Fault-tree (i.e. GAP and CRP) can easily be extended to cover the case of the set of *N* Fault-trees associated with the same safety level or with different safety levels. In the first case the unique goal for frequency reduction (P_G) is defined, whereas in the second case each *j*-th Fault-tree has its own goal P_{Gj}. The effect of any design modification adopted on a selected component belonging to one or more Fault-trees can be assessed also on all the other Fault-trees containing the same component.

3.2.2 Global Importance Indexes

The definition of the different importance indexes applied to a single Fault-tree (defined as *local indexes*) can be extended to the case of the union of two or more Fault-trees. This is essential for implementing CISA as the analysis is conducted concurrently on all Fault-trees. The importance index determined on a set of Fault-trees will be referred to as *global index*. Global importance indexes will be indicated as G followed by the symbol of the importance index for a single Fault-tree.

In this section the equations for determining each global index as a function of the corresponding local indexes are described. This allows determining the global indexes by combining the results obtained from the independent analysis of all Fault-trees.

The notation used is as follows.
Let $\Phi(\mathbf{x}) = \bigcup_{j=1}^{N} \phi_j(\mathbf{y}_j)$ be a logical function consisting of the union on *N* Fault-trees and $\mathbf{x} = \bigcup_{j=1}^{N} \mathbf{y}_j$

where **x** is the vector of all events belonging to all Fault-trees whilst $\mathbf{y}_j$ is the subset of **x** containing all events belonging to the *j*-th Fault-tree.

Hence:

$$\Pr[\Phi(\mathbf{x}) = 1, t] = \sum_{j=1}^{N} \Pr[\bigcup_{j=1}^{N} \phi_j(\mathbf{y}_j) = 1, t] \leq \sum_{j=1}^{N} Q_j$$

More precisely $Q_T = \sum_{j=1}^{N} Q_j$ is a conservative value, which is acceptable under the conditions of the applicability of the rare event approximation method, i.e. the probability of each fault tree is low and their mutual dependence is weak.

Under the same conditions it is acceptable to assume: $Q_{T1k} = \sum_{j=1}^{N} Q_{j1k}$ and $Q_{T0k} = \sum_{j=1}^{N} Q_{j0k}$ (3.6)

Note that under the hypothesis of the applicability of the rare event approximations, a slightly better approximation for Q_T can be obtained applying the Esary-Proschan bound. According to this bound:

$$Q_T \geq 1 - \prod_{j=1}^{N} [1 - Q_j]$$

$$Q_{T1k} \geq 1 - \prod_{j=1}^{N} [1 - Q_{j1k}] \qquad \text{and} \qquad Q_{T0k} \geq 1 - \prod_{j=1}^{N} [1 - Q_{j0k}]$$

Global Birnbaum importance index, GIB

According to the general definition, the Global Birnbaum index of the *k*-th component/basic event is given by:

$$GIB_k = Q_{T1k} - Q_{T0k}$$

As described in the above equation, the Birnbaum importance index IB_k is the probability that a generic component x_k is critical, i.e:

- the system fails if the component fails ($x_k = 1$ implies $\Phi(1_k, \mathbf{x}) = 1$);
- the system works if the component works ($x_k = 0$ implies $\Phi(0_k, \mathbf{x}) = 0$).

Let x_k be a variable belonging to one or more Fault-trees ϕ_j; the **Local Birnbaum index** of the *k*-th event with reference to the *j*-th Top-event (i.e. $\phi_j(\mathbf{y}_j)$) is given by:

$$IB_{jk} = Q_{j1k} - Q_{j0k}$$

If $x_k \notin \mathbf{y}_j$ then $Q_{j1k} = Q_{j0k}$ and $IB_{jk} = 0$.

Since:

$$\Phi(x) = \bigcup_{j=1}^{N} \phi_j(\mathbf{y}_j),$$

it follows that:

$$GIB_k = \Pr\left[\bigcup_{j=1}^{N} \phi_j(1_k, \mathbf{y}_j)\right] - \Pr\left[\bigcup_{j=1}^{Ns} \phi_j(0_k, \mathbf{y}_j)\right]$$

$$\cong \sum_{j=1}^{N} Q_{j1k} - \sum_{j=1}^{N} Q_{j0k}$$

$$\cong \sum_{j=1}^{N} (Q_{j1k} - Q_{j0k}) \cong \sum_{i=1}^{N} IB_{jk}$$

Therefore:

$$GIB_k \cong \sum_{j=1}^{N} IB_{jk}` \quad (3.7)$$

The right-hand side of eq. (3.7) represents an upper bound for the Global Birnbaum index, and it is often a very good approximation thereof. As long as the rare event approximation introduces only a very small conservative error (i.e., the total occurrence probability of the system can be practically expressed as the sum of the occurrence probability of the Top-events), eq. (3.7) becomes:

$$GIB_k = \sum_{j=1}^{N} IB_{jk} \quad (3.8)$$

This condition is generally satisfied due to the quasi-independence of Top-events (i.e. the limited number of common events and the validity of the rare event approximation). In such a situation the probability of simultaneous occurrence of two or more Top-events is negligible.

Global Criticality importance, GIC

The Global Criticality importance index GIC_k of the *k*-th component/basic event for the *N* Fault-trees and the Local Criticality index IC_{jk} of the *k*-th component/basic event for the *j*-th Fault-tree can be simply derived from the Birnbaum index, i.e.:

$$GIC_k = GIB_k \frac{q_k}{Q_T} \quad \text{(Global Index);}$$

Substituting GIB_k with eq. (3.8):`

$$GIC_k \cong \frac{1}{Q_T} \sum_{j=1}^{N} IB_{jk}\, q_k$$

By artificially multiplying by $\frac{Q_j}{Q_j}$ we get:

$$GIC_k \cong \frac{1}{Q_T} \sum_{j=1}^{N} IC_{jk}\, Q_j \quad (3.9)$$

where the right-hand side represents an upper bound for the Global Criticality Index of the *k*-th component/event expressed in terms of the local criticality indexes of the same component. As for the previous case, it often represents also a very good approximation of the index and eq. (3.9) turns into:

$$GIC_k = \frac{1}{Q_T} \sum_{j=1}^{N} IC_{jk}\, Q_j \quad (3.10)$$

If $x_k \notin \mathbf{y}_j$ then $IC_{jk} = 0$, since $IB_{jk} = 0$.

Global Risk Achievement Worth, $GRAW_k$

The $GRAW_k$ is defined as a measure of the change of the system failure probability when x_k is set to 1 in all Fault-trees in which it appears.

$$GRAW_k = \frac{Q_{T1k}}{Q_T} = \frac{\sum_{j=1}^{N} Q_{j1k}}{Q_T}$$

by artificially multiplying the numerator by $\frac{Q_j}{Q_j}$ we get:

$$GRAW_k = \frac{1}{Q_T} \sum_{j=1}^{N} RAW_{jk}\, Q_j \tag{3.11}$$

If $x_k \notin \mathbf{y}_j$ then $RAW_{jk} = 1$.

Global Risk Reduction Worth, $GRRW_k$

The $GRRW_k$ equation as a function of the RRW_{jk} of the component x_k in the N Fault-trees can be derived in a way similar to the one above described for $GRAW_k$, i.e.:

$$GRRW_k \cong \frac{Q_T}{\sum_{j=1}^{N} Q_{j0k}} = \frac{1}{\frac{\sum_{j=1}^{N} Q_{j0k} \frac{Q_j}{Q_j}}{Q_T}} = \frac{1}{\frac{\sum_{j=1}^{N} \frac{1}{RRW_{jk}} Q_j}{Q_T}}$$

$$GRRW_k \cong \frac{Q_T}{\sum_{j=1}^{N} \frac{Q_j}{RRW_{jk}}} \tag{3.12}$$

If $x_k \notin \mathbf{y}_j$ then $RRW_{jk} = 1$

Global Fussell-Vesely importance measure

The GFV_k can be obtained as follows.

$$GFV_k \cong \frac{Q_T - Q_{T0k}}{Q_T}$$

Substituting the equations for Q_T and Q_{T0k} :

$$GFV_k \cong \frac{\sum_{j=1}^{N} Q_j - \sum_{j=1}^{N} Q_{j0k}}{\sum_{j=1}^{N} Q_j} = \frac{1}{Q_T} \sum_{j=1}^{N} \frac{(Q_j - Q_{j0k})\, Q_j}{Q_j} = \frac{1}{Q_T} \sum_{j=1}^{N} FV_{jk}\, Q_j$$

$$GFV_k \cong \frac{1}{Q_T} \sum_{j=1}^{N} FV_{jk}\, Q_j \tag{3.13}$$

If $x_k \notin \mathbf{y}_j$ then $FV_{jk} = 0$.

Global Differential Importance measure **DIM_k**

The $GDIM_k$ importance measure is obtained as follows.

$$GDIM_k = \frac{\frac{\partial Q_T}{\partial q_k} dq_k}{\sum_{i \in x} \frac{\partial Q_T}{\partial q_i} dq_i}$$

By assuming uniform changes in the variables:

$$dq_i = dq_j \quad \forall i, j \in \{x\}$$

the corresponding expression of DIM (H1 suffix) becomes:

$$GDIM_k^{H1} = \frac{\frac{\partial Q_T}{\partial q_k}}{\sum_{i \in x} \frac{\partial Q_T}{\partial q_i}} = \frac{\frac{\partial \sum_{j=1}^{N} Q_j}{\partial q_k}}{\sum_{i \in x} \frac{\partial \sum_{j=1}^{N} Q_j}{\partial q_i}} = \frac{\sum_{j=1}^{N} \frac{\partial Q_j}{\partial q_k}}{\sum_{i \in x} \sum_{j=1}^{N} \frac{\partial Q_j}{\partial q_i}} = \frac{\sum_{j=1}^{N} IB_{jk}}{\sum_{i \in x} \sum_{j=1}^{N} IB_{ji}}$$ resulting in:

$$GDIM_k^{H1} = \frac{GIB_k}{\sum_{i \in x} GIB_i} \tag{3.14}$$

whilst by assuming proportional changes in the parameters i.e.:

$$\frac{dq_i}{q_i} = \frac{dq_j}{q_j} \quad \forall i, j \in \{x\}$$

the corresponding expression of DIM (H2 suffix) becomes:

$$GDIM_k^{H1} = \frac{\frac{\partial Q_T}{\partial q_k} dq_k \frac{q_k}{q_k}}{\sum_{i \in x} \frac{\partial Q_T}{\partial q_i} dq_i \frac{q_i}{q_i}} = \frac{\frac{\partial \sum_{j=1}^{N} Q_j}{\partial q_k} q_k}{\sum_{i \in x} \frac{\partial \sum_{j=1}^{N} Q_j}{\partial q_i} q_i} = \frac{\sum_{j=1}^{N} \frac{\partial Q_j}{\partial q_k} q_k}{\sum_{i \in x} \sum_{j=1}^{N} \frac{\partial Q_j}{\partial q_i} q_i} = \frac{\sum_{j=1}^{N} IB_{jk}\, q_k}{\sum_{i \in x} \sum_{j=1}^{N} IB_{ji} q_i}$$

By multiplying by both the numerator and denominator by $\frac{Q_T}{Q_j}$ the following equation is obtained:

$$GDIM_k^{H2} = \frac{GIC_k}{\sum_{i \in x} GIC_i} \tag{3.15}$$

3.2.3 Concurrent Analysis

As for the single Fault-tree case, the objective of the Goal Achievement Phase (GAP) and Cost Reduction Phase (CRP) is:
1) to reduce the Top-events' occurrence probability to an acceptable value in term of their contribution to risk; and
2) to identify those components that are uselessly reliable, which lead to Top-events' occurrence probabilities that may be far below the established goal.

The main difference, if compared to the single Fault-tree case described in the previous chapter, is the necessity of defining different probability goals (P_{Gj}) for the different Fault-trees, depending on their specific contribution to risk. As the contribution to risk of each Top-event can be displayed in a risk-plot (see Figure 1), a possible criterion to assign the goals (P_{Gj}) is to select values that take the corresponding risk points to an acceptable level. Hence the analysis is based on a multi-goal structure.

The procedure for multiple Fault-trees is very similar to what described in the previous section. In particular, the Concurrent ISA can be applied as if the *N* Fault-trees were descendants from an OR gate of the fictitious Top-event defined as: "*Occurrence of any accident in the plant*". When a given design modification is adopted, then from the *N* Fault-trees those containing the involved component are analysed to determine the impact on all Top-events occurrence probability.

First of all it is necessary to analyse all Fault-trees to obtain the initial values Q_j^0 at step-0 and to compare these values with the probabilistic goals to be achieved. Before that any modification of the system takes place, the occurrence probability of some Top-events could already satisfy the goal condition (i.e. $Q_j^0 \leq P_{Gj}$). In such a case, these Top-events are excluded from the analysis and they are flagged as "**passive**". The concurrent analysis is then conduced only for the system's Top-events that do not satisfy the goal condition, which are referred to as "**active**" Fault-trees. Therefore the N system's fault trees can be subdivided into N_a active and N_p passive trees.

From this point on, the analysis starts by selecting the component/event having the highest global importance index. This component is suitably replaced by another component or subsystem with lower failure probability. At this stage, the recalculated probability of the Top-events are compared with the associated goals, and those Top-events that reach the goals - as a consequence of the introduced modification - are now flagged as "passive" and are excluded from the next steps. The process continues iteratively until all Top-events become "passive", which means that all goals are achieved. Clearly, within the process sequence, several components can be involved in this redesign. It is important to highlight that, at any step of the process, any modification to the system (i.e. improvement of the reliability properties of components of the sequence), cannot alter the goal achievement status of the passive Top-events. This is valid for all coherent system, since the improvement of the reliability of a component cannot but improve the reliability of the system.

Once a modification of the component is made, it is necessary to re-analyse all N fault trees containing the modified event. In order to avoid re-analysing all Fault-trees, it is possible to apply an equation similar to eq. (3.4) that relates the unavailability $Q^{(i)}$ of the system at step-*i* of the modification sequence, to its unavailability at the previous step $Q^{(i-1)}$. Always in the hypothesis of applicability of the rare event approximation method, the unavailability of the system at step (*i*) can be expressed in terms of the unavailability of the Top-events at she same step, i.e.:

$$Q_T^{(i)} = \sum_{j=1}^{N} Q_j^{(i)} \qquad (3.16)$$

As the Top-events' probability values are typically low, the probability of the intersection of two Fault-trees is negligible. By introducing in eq. (3.16) the $Q_j^{(i)}$ expression given in (3.4) it follows that:

$$Q_T^{(i)} = \sum_{j=1}^{N} Q_j^{(i)} = \sum_{j=1}^{N} Q_j^{(i-1)} \left[1 - IC_{jk}^{(i-1)} \frac{(q_k^{(i-1)} - q_k^{(i)})}{q_k^{(i-1)}}\right]$$

where $IC_{jk}^{(i-1)}$ is the local Criticality Index for component *k*-th at the step *i*-1.

By using the relationship between the Local Criticality index and the Global Criticality index (eq. 3.10) and after a little algebra:

$$Q_T^{(i)} = Q_T^{(i-1)}\left[1 - GIC_k^{(i-1)} \frac{(q_k^{(i-1)} - q_k^{(i)})}{q_k^{(i-1)}}\right] \qquad (3.17)$$

which is the equation (3.4) with the Global Criticality Index IC_k instead of the Local Criticality Index IC_{jk}. This expression allows obtaining the value of the system failure probability after a design modification, without re-analysing all involved Fault-trees.

Analogously to the previous single FT case, it is possible to define some parameters, which provide some information about the effectiveness of the system's modification. In particular, the **Global Gain percentage** at the generic *i*-th step, indicated as $G^{(i)}$ and the percentage effort $E^{(i)}$ still to be done to reach the goal are given by:

$$G^{(i)} = \sum_{j=1}^{Na} \frac{Q_j^{(0)} - Q_j^{(i)}}{Q_j^{(0)} - P_{G\,j}} 100 \; ; \qquad E^{(i)} = 100 - G^{(i)} \qquad (3.18)$$

where $Q_j^{(0)}$ is the occurrence probability of the *j*-th Top-event before that any modification takes place, whilst $Q_j^{(i)}$ is the value for the *j*-th Top-event at the *i*-th step resulting from the introduced modification. The sums are extended to the whole set of active Fault-trees.

Analogously, The gain at the generic *i*-th step, referred to as **Global Step Gain percentage** and represented as $\Delta^{(i)}$, is given by:

$$\Delta^{(i)} = \sum_{j=1}^{Na} \frac{Q_j^{(i-1)} - Q_j^{(i)}}{Q_j^{(0)} - P_{G\,j}} 100 \; . \qquad (3.19)$$

It should be noted that, differently from the one-Fault-tree case, the overall goal is not necessarily satisfied when $G^{(i)} \geq 100$, but when $G_j^{(i)} \geq 100 \;\; \forall j \, (j = 1, N_a)$. This means that in the multiple Fault-tree case $G^{(i)} \geq 100$ x N_a (number of active Fault-trees) is a necessary but not sufficient condition to meet the overall goal. If the overall goal is not met then $G^{(i)}$ can not be used for comparison of different intermediate modifications.

It is possible to make the Global Gain percentage more effective by introducing two modifications:

1) limit the total gain taken into consideration for one Fault-tree to 100,
2) normalise the index by the number of active Fault-trees.

As a result of the introduced modifications we have that the **Relative Gain percentage** is given by:

$$RG^{(i)} = \frac{1}{N_a} \sum_{j=1}^{Na} \min\left\{ \frac{Q_j^{(0)} - Q_j^{(i)}}{Q_j^{(0)} - P_{G\,j}} 100, \quad 100 \right\} \tag{3.20}$$

The Relative Gain percentage is expressed as percentage between 0 (initial conditions) and 100% (all Fault-trees satisfies their established goals). The main advantage of this index is that it allows to explicitly rank all the modification sequences having at least one Fault-tree that does not satisfy its probabilistic goal. However it is clear that this index can not be applied to rank modifications where all Fault-trees meets the predefined probabilistic goals (e.g. $RG^{(i)} = 100$ for all possible modification sequences). So the Relative Gain percentage is more suitable in the GAP phase whereas the Global Gain percentage is more suitable to the CRP phase.

4. IMPLEMENTATION OF THE CISA METHOD

The present section provides a very general description of the key aspects of the CISA software developed at the JRC to implement Importance and Sensitivity Analysis applied to multiple Fault-trees. The main features of this tool are hereunder listed:

1) and system modifications on multiple Fault-trees conducted concurrently.
2) Probabilistic analysis of Fault-trees after the introduction of any modification on basic events. These calculations are performed by using the ASTRA BDD module.
3) of different importance indexes (local and global): Criticality index, Birnbaum index, Differential importance measure, Risk achievement worth, Risk reduction worth, Fussell-Vesely, and DIM.
4) Calculation of gain indexes (total gain, step gain, relative gain).
5) Display of all the above results on charts or tables.
6) Automatic recalculation of affected decision tree part in case of intermediate node removal.
7) Check for probabilistic goal achievement and automatic/manual change of Fault-trees status (Active/Passive).
8) Management of the different design alternatives by means of a decision tree.
9) Library of redundant configurations.

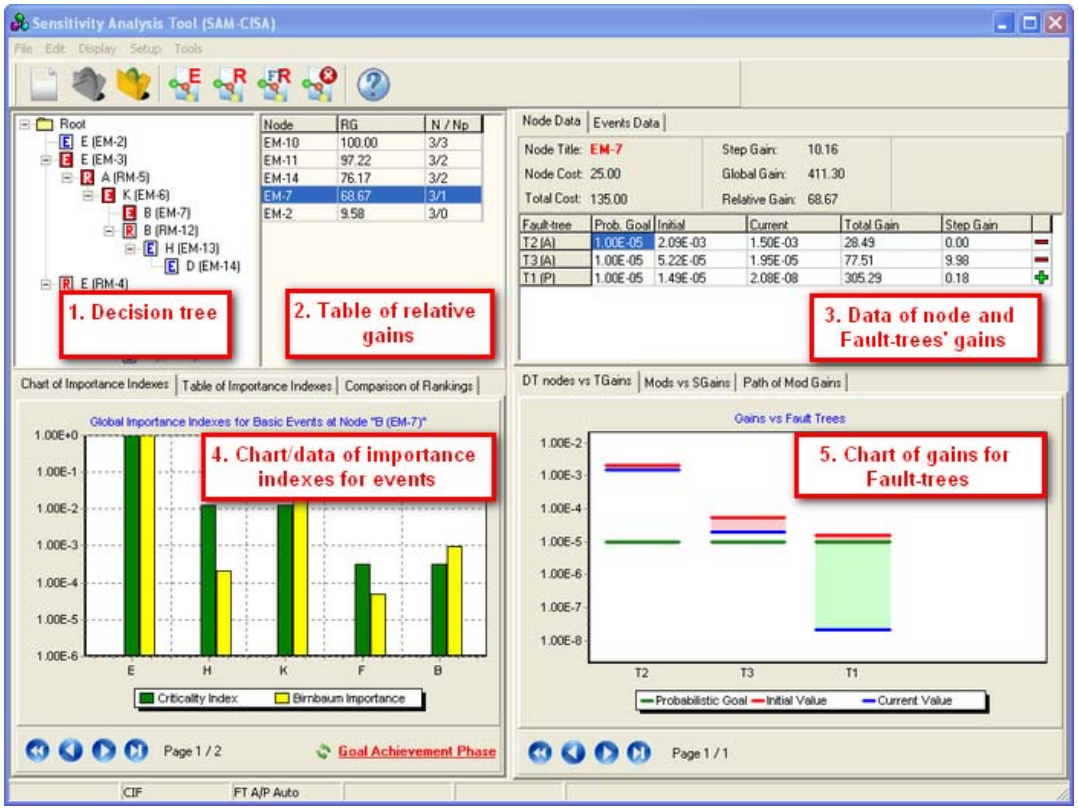


Figure 6: Main window of CISA

The CISA main window is divided into 5 main parts (see Figure 6). The key part is located on the upper-left-side, is indicated with number 1, and referred to as Decision Tree (DT). This is the heart of the user interface, as it is employed in the CISA analysis to manage the different design alternatives and to graphically represent them (see Figure 7).

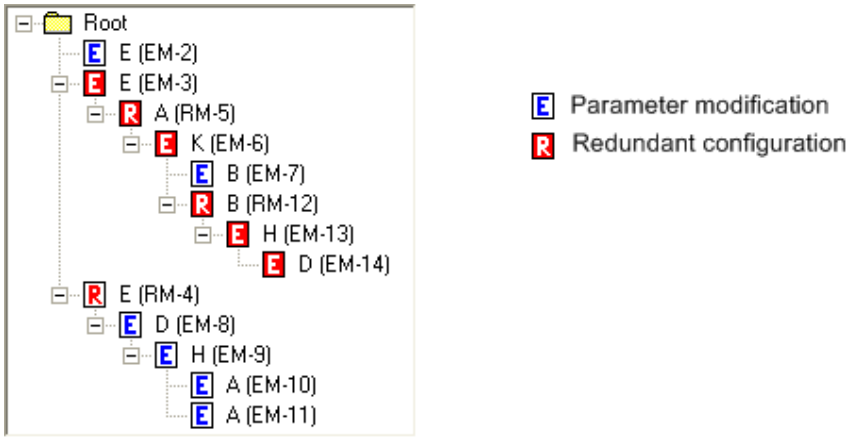


Figure 7: Decision Tree

The decision tree provides the hierarchical structure of the process. The "Root" node is always at the top; it represents the initial system configuration status. Each other node refers to any single modification to the system (the node title consist of the modified component name and unique identification). The path from the selected node to the Root node represents the set of modifications applied to the initial system configuration. As an example, the set of modifications associated with the selected node (EM-14) is highlighted in red (Figure 7).

The first step in the analysis is the selection of component to be modified. Selection process is based on different importance measures. During the analysis the Local Importance Index (LII) is calculated for each component in each of the relevant Fault-trees. Specifically, within each Fault-tree, LII is a relative parameter providing a measure on how a certain component is critical if compared to the others. Clearly such an index will vary for each component submitted to modification during the various steps of the system improvement process. Based on LII, a Global Criticality index (GCI) is then calculated for each component. This global index takes into account of the role played by a certain component in the different Fault-trees in which it is contained. The component whose global criticality index is the highest should generally be taken as first candidate for modifications. An example of chart with different global importance indexes calculated by CISA is presented in Figure 8.

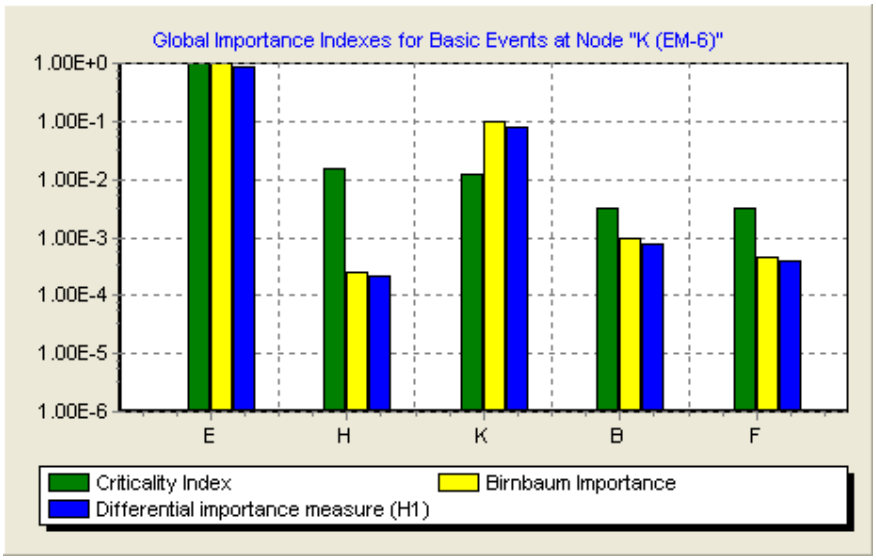


Figure 8: Example chart of global importance indexes

CISA provides analyst with the components ranking table based on selected importance measure (see Figure 9). All components are ranked in descending order according to the selected importance measure. A point to note is that the user can select which specific type of importance indexes should be used and displayed by CISA. Abbreviation of the used importance index for ranking is provided in brackets.

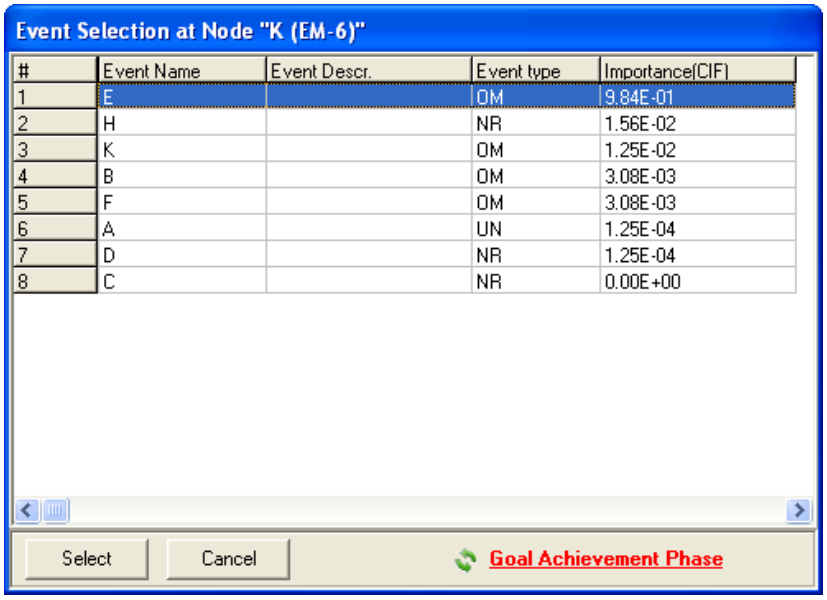


Figure 9: Components ranking table

As a general practice, a new node is normally included in the decision tree, when two modification types are made for the selected component:

1) Change in the component's parameters;
2) Introduction of a redundancy (fault tolerance) by increasing the availability of the component's function.

Modifications are introduced using dialog windows. CISA has two dialog windows – one for each type of modification. CISA dialog window for modification of component's parameters (i.e. 1) is presented in
Figure 10. This window displays all available parameters and allows their modification. After the modification is confirmed the introduced changes are automatically applied to all Fault-trees under investigation and probabilities of all affected Top-events are recalculated.
In order to get a preliminary impact assessment on the modification made, a "preview" function is implemented at the bottom of the dialog. New Top-event probabilities are obtained by using the value of the probability at the previous step according to the equation (3.4) without re-analysing the Fault-tree. Re-analysis of Fault-trees is performed only after the modification is confirmed.

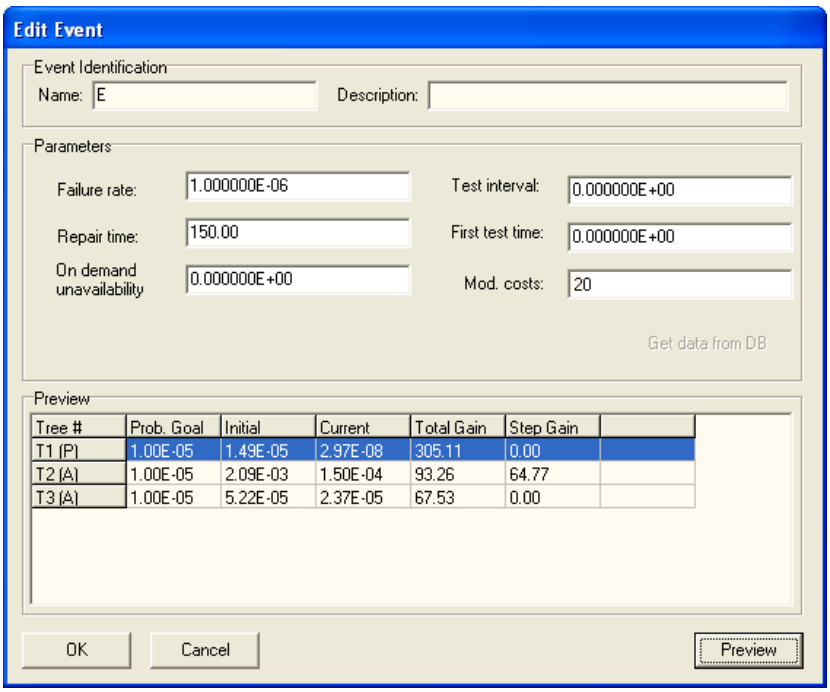


Figure 10: Window for modification of component's parameters

The dialog for redundancy modification (i.e. 2) is given in Figure 11. Different redundancy types can be applied using this dialog without modification of the Fault-tree structure (parallel, K/N of active events, K/N of tested events, etc.). Same "preview" function is foreseen to estimate preliminary modification impact to the Top-events without performing a complete re-analysis of Fault-trees.

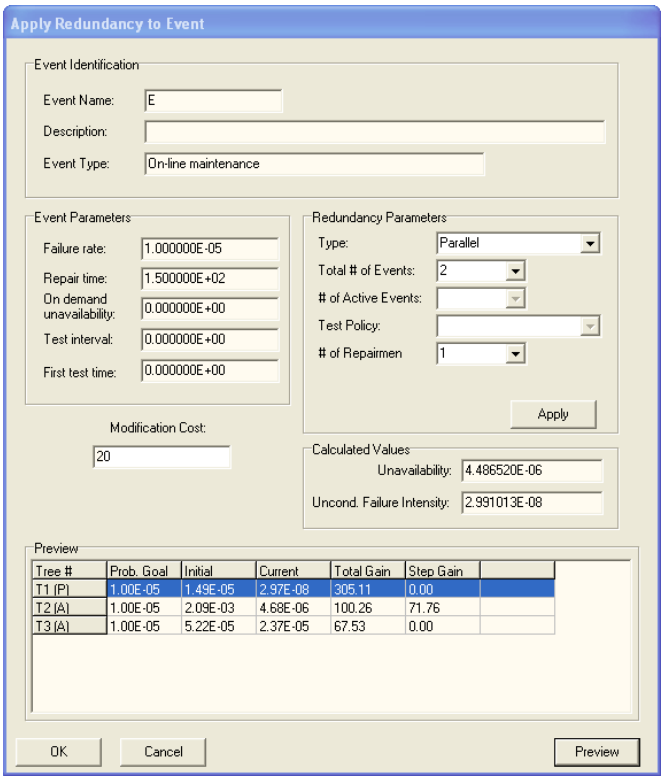


Figure 11: Window for redundancy modification

CISA software automatically updates all affected Fault-trees after the modification phase is finished off and the probabilistic analysis is reprocessed. As a result, new intermediate occurrence probabilities for Top-events are obtained. These are normally better than previously and, in turn, the pre-defined probabilistic goals are approached. The Relative Gain value (a number between 0 and 100) is calculated taking into consideration the user-defined goal (desired Top-event occurrence rate) and the actually reached top-event occurrence rate. After some modifications, the user eventually decides whether the improvement of the system is acceptable or not. To support the decision making process CISA provides the user with different types of information.

The general outcome of the analysis is shown in sub-windows 2-5 of the main CISA window (see Figure 6). For each end node of the decision tree: the Relative Gain index, the total number of Fault-trees, and the number of Fault-trees that have already reached their predefined goals is displayed (Figure 12).

Node	RG	N / Np
EM-10	100.00	3/3
EM-11	97.22	3/2
EM-14	76.17	3/2
EM-7	68.67	3/1
EM-2	9.58	3/0

Figure 12: Example of results representation for decision tree end nodes

Additionally, the CISA software provides calculation results for all Fault-trees in the selected node of the decision tree. The information is listed in tables and displayed on charts. Some examples of results representation are given in
Figure 13 (Global, relative and step gains for the selected DT node and gain representation for each of the Fault-trees) and Figure 14 (graphical representation of gains for each of the Fault-trees).

Node Data | Events Data

Node Title: EM-6 Step Gain: 67.53
Node Cost: 30.00 Global Gain: 401.14
Total Cost: 110.00 Relative Gain: 65.34

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T2 (A)	1.00E-05	2.09E-03	1.50E-03	28.49	0.00	−
T3 (A)	1.00E-05	5.22E-05	2.37E-05	67.53	67.53	−
T1 (P)	1.00E-05	1.49E-05	2.97E-08	305.11	0.00	+

Figure 13: Example of results representation for selected decision tree node

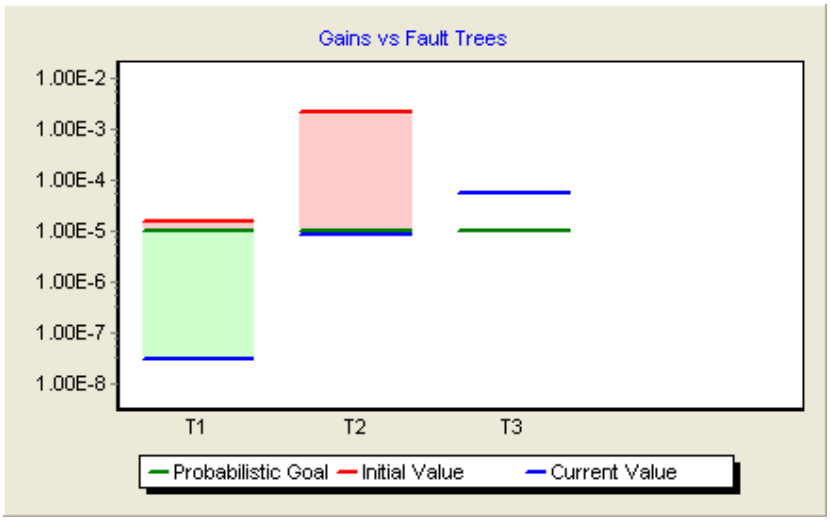


Figure 14: Example of results chart representing gains for decision tree nodes

In order to compare impact of different modifications to the system under investigation – the chart of step gains is generated by CISA (Figure 15). It provides all the nodes of the decision tree ordered in descending order according the step gains.

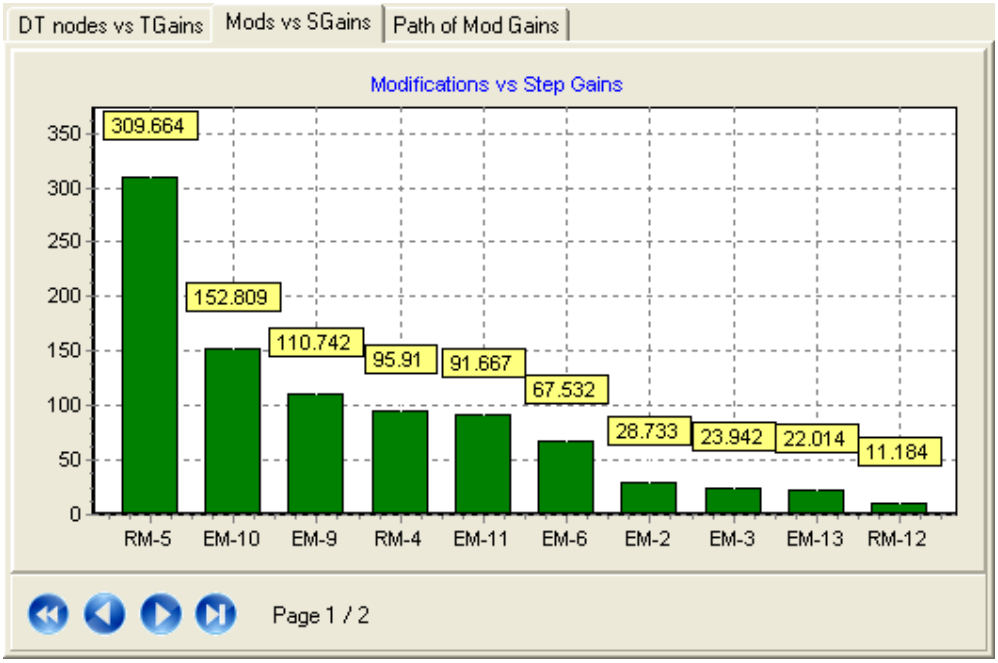


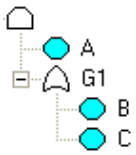
Figure 15: Example of results chart representing step gains for different modifications

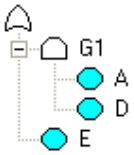
The use of CISA software gives to the analyst the possibility to perform an analysis of possible system modifications and it allows examining the possible different ways to improve the system and to optimise the costs.

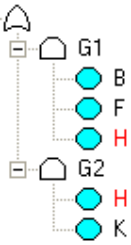
5. APPLICATION EXAMPLE

5.1 Problem Definition

The methodology described in the previous section is applied to the case of three Fault-trees, which are supposed to be associated with the same safety level and having the same goal $P_G = 10^{-5}$ for risk reduction. The logical functions of the three Fault-trees are given below.







TOP_1 = A B + A C **TOP_2 = A D + E** **TOP_3 = B F H + H K**

TOP_1 and TOP_2 contain the common basic event A; TOP_1 and TOP_3 contain the common event B.

The basic events data are given in Table 2, where λ represents the failure rate and τ the repair time. The last row contains the BE's unavailability q(t) at mission time t = 10,000 hours.

BE	A	B	C	D	E	F	H	K
λ(h^{-1})	10^{-5}	10^{-4}	10^{-6}	10^{-5}	10^{-5}	10^{-4}	10^{-5}	10^{-5}
τ(h)	100	50	-	-	200	100	-	50
q(t)	$9.99\cdot10^{-4}$	$4.97\cdot10^{-3}$	$9.95\cdot10^{-3}$	$9.51\cdot10^{-2}$	$1.99\cdot10^{-3}$	$9.90\cdot10^{-3}$	$9.51\cdot10^{-2}$	$4.99\cdot10^{-4}$

Table 2: Main parameters associated with the BE of the reference system (initial design configuration)

Initially, the analysis of the above Fault-trees will be performed by applying the SISA method, i.e. by analysing the Fault-Trees sequentially. Then the concurrent sensitivity analysis will be performed using the CISA approach and the related software. Finally, the results of the two approaches will be compared and discussed. Use is made of the Criticality index as BE importance measure.

5.2 System analysis using the SISA approach

The Sequential ISA applied in this example considers each Fault-tree independently, but the analysis of a given Fault-tree in the sequence takes into account the design modifications adopted on the previously analysed Fault-trees. ASTRA 3.0 is the tool used for the calculations.

Analysis of TOP_1

The analysis of FT_1, with the BE data in Table 2, gives the following results: Q_1 = 1.49E-5.

The Criticality importance indexes for this case are as follows:

BE	IC
A	1.0
C	0.665
B	0.331

A is clearly the most important component. By supposing that on this component it is possible:

- to apply active redundancy at a cost of 15 units;

- to reduce the repair time to 50h through design changes at a cost of 10 units.

The approach to follow is always to adopt the least expensive solutions, provided that they allow satisfying the goal. The re-running of FT_1 after modifying the repair time of A to 50 h gives the new result: $Q_1 = 7.43E\text{-}6$.

Since $Q_1 < P_G$ the goal is achieved for FT_1 at a cost of 10 units.

Analysis of TOP_2

The analysis of FT_2 is performed by using the data in Table 2 with the exception of data for component A for which the repair time is now 50 h instead of 100h. In other words, before analysing FT_2 it is convenient to make the modifications identified from the analysis of FT_1. With such a modification the analysis of FT_2 leads to $Q_2 = 2.04E\text{-}3$, which is still far from satisfying the goal.

The corresponding Criticality importance indexes of the basic events are as follows:

BE	IC
E	0.976
A	2.32E-2
D	2.32E-2

The most important component is E.

Suppose that on this component it is possible:

- to apply active redundancy at cost of 10 units;
- to reduce the repair time to 150 h through design changes at a cost of 5 units.

Again the least expensive solution is considered. Re-running FT_1 after having modified the repair time of E gives the new result: $Q_2 = 1.59E\text{-}3$, which is absolutely not effective. Thus, redundancy on E is then applied (E is substituted with E1 $\wedge$ E2). In order to obtain results coherent with those given by CISA the calculation has been performed off-line considering one repairman (N=2 and R=1, see Appendix). In this case $Q_2 = 4.98E\text{-}5$, which represents a very good improvement, but not sufficient to achieve the goal. With this new design configuration the importance indexes become:

BE	IC
A	0.922
D	0.922
E1	7.73E-2
E2	7.73E-2

Now the most important components are A and D. The event A was already considered in FT_1. The following design alternatives are possible:

- to use the redundancy for A (cost = 15);
- to make D repairable with mean repair time of 200h at a cost of 15 units.

Hence both alternatives are feasible. For instance making D repairable gives: $Q_2 = 8.96E\text{-}6$ (the alternative, i.e. to make A redundant does not give a significant difference).

Analysis of TOP_3

The analysis of FT_3 is performed by using the data in Table 2 and the new data for E, A as resulting from the analysis of FT_1 and FT_2.

BE	A1,A2	B	C	D	E1, E2	F	H	K
λ(h^{-1})	10^{-5}	10^{-4}	10^{-6}	10^{-5}	10^{-5}	10^{-4}	10^{-5}	10^{-5}
τ(h)	50	50	-	-	200	100	-	50

Table 3: Main parameters associated with the BE of the reference system (after the analysis of FT_1 and FT_2)

Under these conditions the analysis of FT_3 gives: Q_3 = 5.22E-5, which does not achieve the goal.

The Criticality importance indexes of the basic events are as follows:

BE	IC
H	1.0
K	0.910
B	8.96E-2
F	8.96E-2

The most important component is H, which has the highest IC followed by K as a good candidate for design improvement.

Suppose that on these components one can:

- make H repairable with mean repair time of 100 h at a cost of 20 units;
- make K redundant at a cost of 30 units.

The first alternative is selected. Consequently, Q_3 = 5.48E-7 which satisfies the goal.

Summarising, the final Top-events values that satisfy the goal P_G =1.0E-5 are:

Q_1 = 7.43E-6;
Q_2 = 8.96E-6;
Q_3 = 5.48E-7,

These results can be obtained by adopting the following solution:

- reduce the repair time of A to 50 h (cost= 10).
- apply active redundancy to E (cost = 10);
- use redundancy for A (cost = 15);
- make H repairable with mean repair time of 100 h (cost= 20);

The total cost is 55.

What has been obtained is one particular solution among the set of possible existing alternatives, but it is not possible to know whether it represents the best in terms of its cost-effectiveness. Certainly it is the best solution according to the selected sequence of examined fault trees (FT_1-FT_2-FT_3) because at each time the cheapest modification was selected. On the other hand, other solutions could also be found by considering different sequences for the Fault-trees under examination. The identified solution is indeed associated with the *order* in which the Fault-trees are analysed. Theoretically, it can be said that given N dependent Fault-trees the number of fault tree sequences is at most N!.
Hence, in order to select the solution with minimum cost it is not sufficient to apply the SISA approach only once, as commonly occurs in practice.

To clarify this concept let's suppose to start the analysis from FT_3, proceeding with FT_2 and finally with FT_1. From the analysis of FT_3 the initial value $Q_3 = 5.22E\text{-}5$ can be decreased to $Q_3 = 5.48e\text{-}7$ by making H repairable with mean repair time of 100h (cost = 20).
The analysis of FT_2 gives $Q_2 = 2.09E\text{-}3$; the most important event is E. Making E redundant reduces the top-event unavailability to $Q_2 = 1.03E\text{-}4$ which, however, does not achieve the goal. Also here the calculation has been performed off-line considering one repairman (N=2 and R=1, see Appendix). The most important events is A; making it redundant (same as for E) reduces the top event probability to $Q_2 = 8.15E\text{-}6$, which achieves the goal. With the above modifications the analysis of FT_1 gives $Q_1 = 2.96E\text{-}8$: this tree does not require any modification.

By summarising:
$Q_1 = 2.96E\text{-}8$;
$Q_2 = 4.07E\text{-}6$;
$Q_3 = 5.48E\text{-}7$,
which can be obtained by adopting the following solution:

- make H repairable with mean repair time of 100 h (cost= 20);
- apply the active redundancy to E (cost = 10);
- use the redundancy also for A (cost = 15);

In this case the total cost is 45.

Compared with the previous analysis (FT_1-FT_2-FT_3) the second sequence (FT_3-FT_2-FT_1) gives a better solution which could never been obtained if the analysis were performed on the first sequence. Indeed, in the practical use of the SISA procedure only one sequence is considered.

5.3 System analysis using the CISA approach

5.3.1 Goal Achievement phase

This section presents the results of system analysis obtained by applying the CISA approach for the example described in section 5.1. All the calculations were performed using the specific CISA software tool.

After having uploaded the input data for the analysis, CISA performs the calculations for the initial system configuration ("Root" node of the decision tree). All these initial calculations are summarised in a dialog table as shown in Figure 16: Probabilistic goals, Initial and Current probabilities for Top-events; clearly Total and Step gains are zero.

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T2 (A)	1.00E-05	2.09E-03	2.09E-03	0.00	0.00	
T3 (A)	1.00E-05	5.22E-05	5.22E-05	0.00	0.00	
T1 (A)	1.00E-05	1.49E-05	1.49E-05	0.00	0.00	

Figure 16: Probabilistic data for the Fault-trees at the "Root" node

As it can be seen from Figure 16 none of these Fault-trees satisfy the goal $P_{G.}$, i.e. they will all be considered as "active" in the following analysis. This is marked by the "minus" red sign in the last column. For each Basic-Event CISA calculates the Criticality indexes as given in Figure 17. The

importance measures are used to rank the events in decreasing order. The last row (denoted as GCI) contains the Global Criticality index value of the basic events present in "active" Fault-trees.

	B	A	C	E	D	H	K	F
T1	0.331	1.000	0.666					
T2		0.045		0.955	0.045			
T3	0.090					1.000	0.910	0.090
GCI	0.004	0.051	0.005	0.925	0.044	0.024	0.022	0.002

Figure 17: Local and Global Criticality indexes of the BE for the reference system

For the initial system configuration the basic event with the highest global importance index is E (0.925) belonging to FT_2 only. Let's suppose, as before, two possible modifications could be conceived for this event representing the failure mode of a repairable component:

Alternative RM-2: Use the parallel redundancy (E1 $\wedge$ E2 substitute E) (cost = 10)
Alternative EM-3: Reduce the repair time of E from 200 h to 150 h (cost = 5)

With these alternatives new values for Q_2 are obtained (Q_1 and Q_3 values are not affected, since they do not contain E):

Alternative RM-2:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T2 (A)	1.00E-05	2.09E-03	1.03E-04	95.53	95.53	
T3 (A)	1.00E-05	5.22E-05	5.22E-05	0.00	0.00	
T1 (A)	1.00E-05	1.49E-05	1.49E-05	0.00	0.00	

Alternative EM-3:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T2 (A)	1.00E-05	2.09E-03	1.59E-03	23.94	23.94	
T3 (A)	1.00E-05	5.22E-05	5.22E-05	0.00	0.00	
T1 (A)	1.00E-05	1.49E-05	1.49E-05	0.00	0.00	

Figure 18: Calculation results after modification of component E

Both alternatives deserve to be retained; however, as expected, the first is more effective as it has a higher Relative Gain percentage value (*Alternative "RM-2"*: RG = 31.84; *Alternative EM-3*: RG = 7.98).

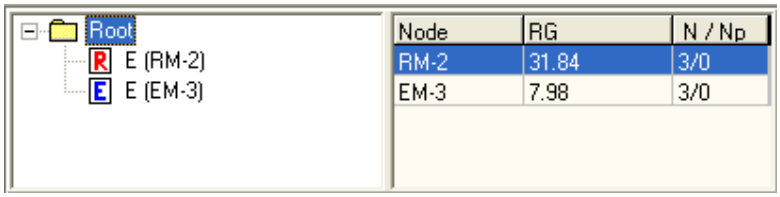


Figure 19: Decision diagram after the first phase of the analysis

At this stage it is necessary to select the alternative to be adopted. This is indicated in the in the decision diagram in which the selected alternative (RM-2) is depicted in red whilst the other (EM-3) is in blue (see Figure 19).

RM-2

In order to proceed with the analysis, new importance indexes for the newly designed system (at decision tree branch "RM-2") have to be considered. In the present case they are given in Figure 20.

	B	A	C	E	D	H	K	F
T1	0.331	1.000	0.666					
T2		0.923		0.077	0.923			
T3	0.090					1.000	0.910	0.090
GCI	0.056	0.646	0.058	0.047	0.559	0.307	0.280	0.028

Figure 20: Local and Global Criticality indexes of the BE for the system as modified via alternative "RM-2"

As it can be seen the most important event is now A (0.646), which is contained in TOP_1 and TOP_2. For the second analysis step two new alternatives can be considered:

Alternative EM-4 : Reduce the repair time of A from 100 h to 50 h (cost = 10)
Alternative RM-5: Use the parallel redundancy (A1 $\wedge$ A2 substitute A) (cost = 15)

With these alternatives new values for Q_1 and Q_2 can be obtained (Q_3 is not affected, since TOP_3 does not contain A):

Alternative EM-4:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T2 (A)	1.00E-05	2.09E-03	5.55E-05	97.81	2.28	−
T3 (A)	1.00E-05	5.22E-05	5.22E-05	0.00	0.00	−
T1 (P)	1.00E-05	1.49E-05	7.43E-06	152.78	152.78	+

Alternative RM-5:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T3 (A)	1.00E-05	5.22E-05	5.22E-05	0.00	0.00	−
T2 (P)	1.00E-05	2.09E-03	8.16E-06	100.09	4.56	+
T1 (P)	1.00E-05	1.49E-05	2.97E-08	305.11	305.11	+

Figure 21: Calculation results after modification of component A

The second alternative is more effective as it has higher Relative Gain index value (*Alternative RM-5*: RG = 66.67; *Alternative EM-4*: RG = 65.94,) as it can be seen from CISA calculations (Figure 21),.

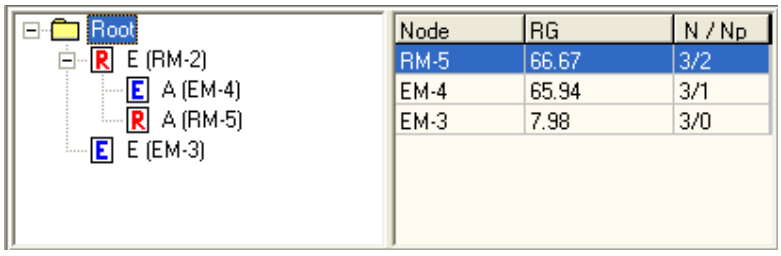


Figure 22: Decision diagram after the second phase of the analysis

With alternative EM-4, one Fault-tree (TOP_1) satisfies the goal condition whilst with alternative RM-5 two of Fault-trees satisfy the goal condition. For this reason the second alternative is selected first for analysis.

RM-5

In this case TOP_1 and TOP_2 satisfy the goal condition ($Q<10^{-5}$), so they will not be considered for further improvement are labelled as "passive" trees (to specify that they will not be considered for the importance indexes' calculation). By contrast, Q_1 and Q_2 are still calculated in order to see how they change as a result of the subsequent design alternatives. In order to proceed with the analysis, the new global importance indexes are determined considering the basic events of the active trees (TOP_3 only in the present example). These values are given in Figure 23. Note that GCI for basic events not belonging to the "active" Top_3 are zero.

	B	A	C	E	D	H	K	F
T1	0.331	1.000	0.666					
T2		0.023		0.977	0.023			
T3	0.090					1.000	0.910	0.090
GCI	0.090	0.000	0.000	0.000	0.000	1.000	0.910	0.090

Figure 23: Local and Global Criticality indexes of the BE for the system as modified via alternative "RM-5"

We notice that as far as TOP_3 is concerned, the most important event is H. Let's suppose that H can be made repairable (modification "EM-6"), whilst redundancy is not feasible due, for instance, to space problems. Suppose that the estimated mean repair time can be reduced to 100 h at a cost of 20. With this modification we find the following results:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain	
T2 (P)	1.00E-05	2.09E-03	8.16E-06	100.09	0.00	
T3 (P)	1.00E-05	5.22E-05	5.48E-07	122.37	122.37	
T1 (P)	1.00E-05	1.49E-05	2.97E-08	305.11	0.00	

Figure 24: Probabilistic data for the Fault-trees after modification "EM-6"

At this point the goal $P_G = 10^{-5}$ is achieved for all Fault-trees (RG = 100), as can be seen from figures 24 and 25.

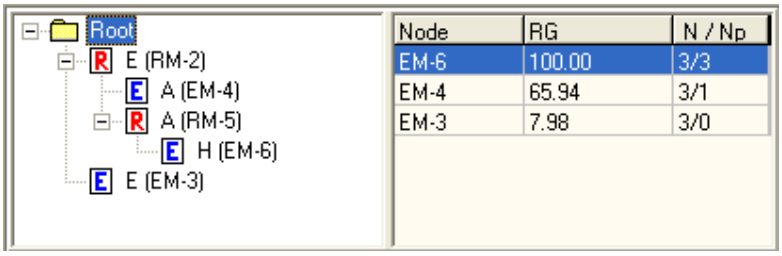


Figure 25: Decision diagram after the third phase of the analysis

Overall, this particular design solution ("EM-6") has been obtained by applying the following modifications:

- to apply the active redundancy to E (cost = 10);
- to use the redundancy for A (cost = 15);
- to make H repairable with mean repair time of 100 h (cost= 20);

The total cost is 45.

EM-4

Now we can go back to the last suspended alternative "EM-4" and proceed with it. After implementing it, one Fault-tree (TOP_1) already satisfies the goal condition so it is labelled as passive. The calculation of the new importance indexes at the node "EM-4" show that the most important event is H. If we apply the very same modification on H as described above (H made repairable with the mean repair time 100 h) it is possible to demonstrate that the second Fault-tree (TOP_2) does not still satisfy the goal condition and an other modification is made necessary. The recalculation of importance indexes leads to the selection of D as the component to modify having this the highest importance. By assuming that this component can be made repairable with estimated repair time of 200 h at a cost of 15, the calculation show that all Fault-trees satisfy their predefined goals.

Overall the final solution ("EM 8") has been obtained by applying the following modifications:

- to apply the active redundancy to E (cost = 10);
- to use the redundancy for A (cost = 15);
- to make H repairable with mean repair time of 100 h (cost = 20);
- to make D reparable with mean repair time of 200 h (cost = 15).

The total cost is 60, which is less convenient than the previous solution.

EM-3

At this point we can now return to suspended decision tree branch "EM-3" (Figure 25) and to assess other possible modification alternatives. From the table of Criticality importance indexes (Figure 26) it can be seen that component E has the highest Criticality index. However this was already considered for improvement and therefore we will proceed with the next most important component A.

	B	A	C	E	D	H	K	F
T1	0.331	1.000	0.666					
T2		0.060		0.940	0.060			
T3	0.090					1.000	0.910	0.090
GCI	0.006	0.066	0.006	0.902	0.057	0.031	0.029	0.003

Figure 26: Local and Global Criticality indexes of the BE for the system as modified via alternative "EM-3"

As for the previous cases, there are two possible alternatives for component A: to introduce the parallel redundancy or to reduce its repair time of from 100 h to 50 h. Calculation results shows that for both modifications the first Fault-tree (TOP_1) reaches the goal. However the other Fault-trees still does not satisfy their predefined goals. As it can be seen from the previous calculations (Figure 21) redundancy modification is more effective. For this reason this alternative first was selected. The further calculation of criticality importance indexes leaded to the selection of H for modification. As it was stated before, the only feasible modification is to make it repairable with repair time 100 h ("EM-11"). With this the third Fault-tree reached the goal whilst the second Fault-tree resulted still with its goal to be attained. As for the second Fault-tree – two out of its three components were already modified (A and E), therefore the only component not-modified left, is D. –As previously stated, component D can be made repairable and the estimated repair time is 200 h ("EM-12"). Nevertheless also with such a modification the second Fault-tree did not still achieve the goal and since the cost of this sequence at

this stage is already 55, which is higher then the previously established sequence ("EM-6" = 45), it was decided that it does not make sense to continue any further.

Using the same approach, the suspended decision tree branch "EM-9" was investigated. Based on the calculated Criticality importance indexes the following modifications were applied:

"EM-13": H was made repairable with estimated repair time 100 h (cost = 20).
"EM-14": D was made repairable with estimated repair time 200 h (cost = 15).

As a result of these modifications Fault-trees TOP1 and TOP3 reached the goals, but Fault-tree TOP2 still failed to reach the predefined goal. Since also in this case the cost of this sequence is already 55, and therefore, higher then the previously established sequence ("EM-6" = 45), it does not make sense to continue any further.

The final decision tree is presented in Figure 27.

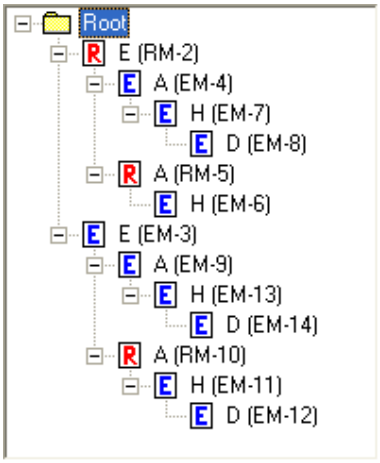


Figure 27: Decision diagram after the last phase of the analysis

As it can be seen from Figure 28 only two out of the four considered modifications reached the predefined goals. The others were abandoned because they were not efficient enough.

Node	RG	N / Np	
EM-8	100.00	3/3	**Cost=60**
EM-6	100.00	3/3	**Cost=45**
EM-12	76.17	3/2	**abandoned**
EM-14	76.15	3/2	**abandoned**

Figure 28: Decision diagram after the last phase of the analysis

A point to note is that, in theory, the analysis on the two sequences which have not achieved the goal can always be continued. However at this stage of the analysis their costs (EM-12 = 55; EM-14 = 55) are already comparable or higher then the costs of the two sequences that are more effective. This is a typical situation that is not necessarily associated with the application example presented in this report.

5.3.2 Cost Reduction Phase

The previous section has shown how the system can be improved in order to achieve the attained goal. However, it might happen that as a result of these modifications one or more functions of the system may result over-protected. The cost reduction phase addresses those components having lowest

importance indexes, which might be associated with "over-reliable" functions in the system. The objective of this phase is to partially relax the reliability/maintainability characteristics of the components associated with these functions that are over protected in order to achieve a system which is uniformly protected.

Let's suppose that the selected design modification is sequence EM-9, which was indicated in the previous section as the most effective. As it can be seen from Figure 29, the goal was reached for all Fault-trees. However the system is clearly overprotected. In particular, the figure compares the occurrence probability of the Top-events (T1, T2, and T3) before the introduced design modifications (**horizontal red bars**), after the modifications indicated by sequence EM-6 (**horizontal blue bars**), and the probability goal (**horizontal green bar**), which for the present case was the same for all Fault-trees. As it can be seen from the figure, there is space for improvement for T1 and T3 (i.e. FT1 and FT3), being their probabilistic values much below the goal (large green areas).

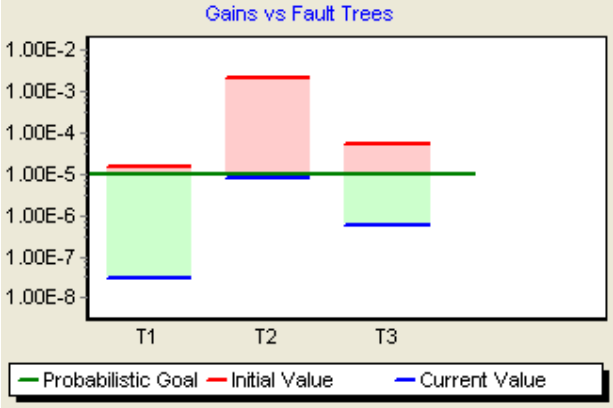


Figure 29: Graphical representation of the probabilistic data for the nodes "EM-6"

The calculations of the BE Criticality indexes for the final system configuration described by the Decision tree node "EM-6" are given in Figure 30. Differently from the Goal Achievement Phase, in the Cost Reduction Phase all Fault-Trees are taken into account, independently of their status for the estimate of Importance indexes. Thus the analysis is not restricted to "active" Fault-Trees.

	B	A	C	E	D	H	K	F
T1	0.331	1.000	0.666					
T2		0.023		0.977	0.023			
T3	0.090					1.000	0.910	0.090
GCI	0.007	0.025	0.002	0.912	0.022	0.063	0.057	0.006

Figure 30: Local and Global Criticality indexes of the BE for the system configuration "EM-6"

As it was already stressed in a previous section, the cost reduction phase is addressed to assess whether some of the less critical components are uselessly reliable and can be worsened in order to obtain a more uniformly reliable system. This means, for instance, that the occurrence probability of TOP_1 ($Q_1 = 2.97 \times 10^{-8}$), which is far below the goal $P_G = 10^{-5}$, could be increased if suitable design modifications can be found.

From Figure 30, it is clear that the non-repairable component *C* is the less critical for the system. By considering a cheaper component with a higher failure rate (e.g. $\lambda = 10^{-4}\ h^{-1}$), it is possible to show that

the corresponding values of Top-events occurrence probabilities will satisfy the goal ($Q<10^{-5}$). Such a modification clearly produces some savings as it makes use of a component that costs 25 units less.

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain
T2 (P)	1.00E-05	2.09E-03	8.16E-06	100.09	0.00
T1 (P)	1.00E-05	1.49E-05	1.27E-06	279.69	-25.42
T3 (P)	1.00E-05	5.22E-05	5.48E-07	122.37	0.00

Figure 31: Probabilistic data for the Fault-trees after modification of component C

Since the gains for FT1 and FT3 are still sensitively higher then 100 there is still space for improvement. By recalculating the importance indexes after the introduced modification, the component *F* resulted in the lowest importance. In particular, *F* is repairable with mean repair time of 100 h. If the mean repair time is increased to 300 h, the corresponding values of Top-events occurrence probabilities will be:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain
T2 (P)	1.00E-05	2.09E-03	8.16E-06	100.09	0.00
T1 (P)	1.00E-05	1.49E-05	1.27E-06	279.69	0.00
T3 (P)	1.00E-05	5.22E-05	6.44E-07	122.15	-0.23

Figure 32: Probabilistic data for the Fault-trees after modification of component F

which is still acceptable. To note that the increase of repair time might have a significant impact on:

i) the spare parts management,
ii) the maintenance organisation.

which have clearly a significant impact on the overall costs.

By proceeding further, the next least important components on this system configuration resulted: *B, D* and *K; B* and *K* are repairable and component *D* is not repairable. The decision to increase the repair time from 50 to 300 h for repairable components *B* and *K* and for component *D* the option to replace it with a cheaper component having higher failure rate (e.g. $\lambda = 10^{-4}$ h^{-1}) was considered. All these actions are clearly associated with cost reductions. Calculations confirmed that Top-event occurrence probabilities are still within the goal range. The corresponding probabilities of the three Top-events have changed as follows:

Fault-tree	Prob. Goal	Initial	Current	Total Gain	Step Gain
T2 (P)	1.00E-05	2.09E-03	9.23E-06	100.04	0.00
T3 (P)	1.00E-05	5.22E-05	3.83E-06	114.60	-5.89
T1 (P)	1.00E-05	1.49E-05	1.28E-06	279.33	0.00

Figure 33: Probabilistic data for the Fault-trees after modification of components B, D and K

which corresponds to a possible new system configurations obtained from reference one (E and A redundant and H made reparable) by substituting *C* and *D* with components of worst quality, and extending the mean repair time of *B, F,* and *K* to 300 h.

The final decision tree and graphical representation of probabilistic data for the Fault-trees after the cost reduction phase of the analysis are presented in Figure 34 and Figure 35.

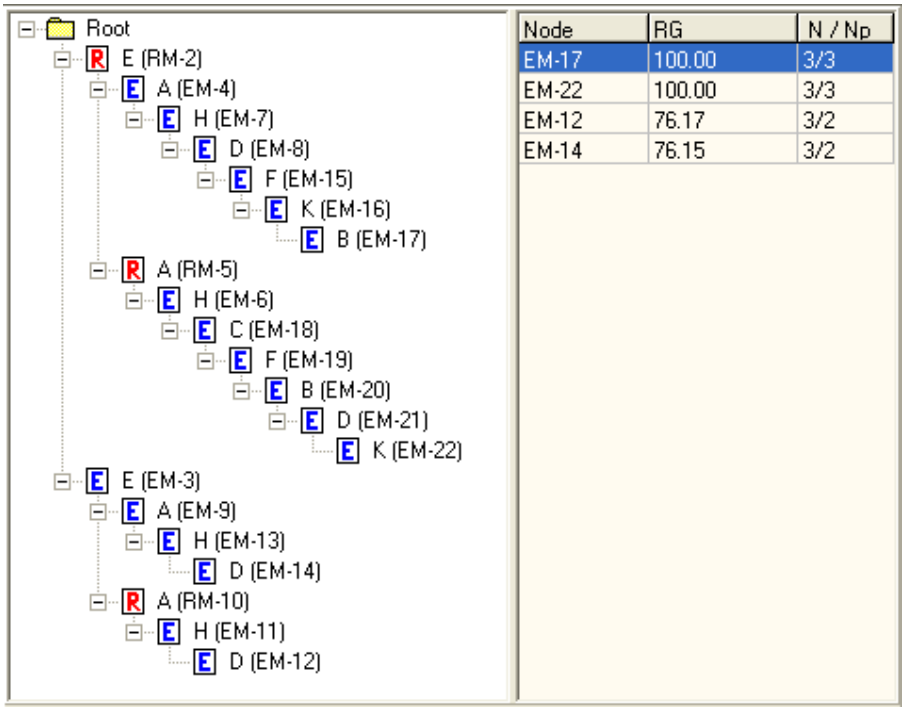


Figure 34: Decision tree after the last phase of the analysis

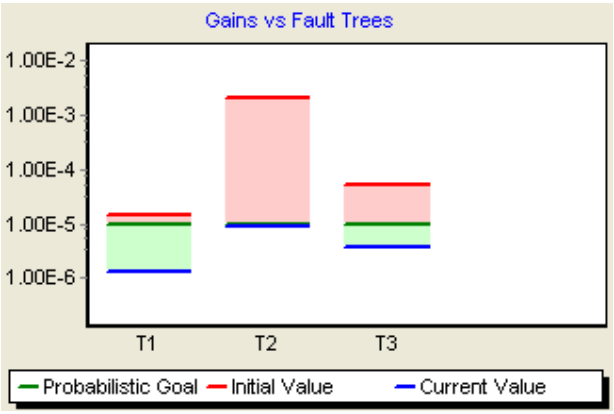


Figure 35: Graphical representation of the probabilistic data for the nodes "EM-6" after the cost reduction phase

5.4 Discussion on results

The comparison of this application exercise executed by using SISA and CISA approaches shows that, in general, the sequential approach allows obtaining a feasible design solution which is not necessarily the most effective as for the CISA case. More specifically, the final design solution that is obtained by using SISA is very much influenced by the considered fault tree sequence. Starting the analysis from a certain Fault-tree or another might easily produce different, acceptable, solutions, which are very likely not the most effective. In addition, normal practice imposes that the analysis conducted on the *k*-th Fault-tree in the sequence is not followed by the re-analysis of all previously analysed Fault-trees. Clearly the only way forward to avoid this problem is to consider different sequences and to re-analyse

all previously analysed Fault-trees containing the modified components. This practice would be, however, too expensive and time consuming.

In the presented example, the sequential approach has allowed to obtain a design sequence where component *A* had to be modified twice to allow the achievement of the goal for the second Fault-tree. It is worth to note that the second modification on *A* would have been sufficient even for the first Fault-tree if the outcome of the second Fault-tree was known a-priori. In such a way the first modification could have been avoided if a re-analysis of the first Fault-tree was conducted after the second.

By contrast this type of difficulty is not present in CISA. Indeed, at each step of the procedure it is possible to select the most "promising" sequence according to the overall gain and cost. The best cost-effective set of modifications can always be identified, whereas this is not guaranteed with the SISA approach.

6. CONCLUSIONS AND ON-GOING DEVELOPMENTS

The present report described the Concurrent Importance and Sensitivity Analysis (CISA) approach for system design improvement using Fault-tree Analysis. The advantage of the method is represented by the possibility to perform the sensitivity analysis for design improvement on all Fault-trees at the same time. This is possible due to the calculations of the global importance indexes of the system's components and the analysis performed on all Fault-trees concurrently, thus giving the designer the effects on the whole system of the applied design modification. The global importance indexes are the basic data that allow the rapid identification of the relatively weakest parts of the system, where better design solutions are needed. Whence the weakest parts are identified, three different types of interventions are possible to improve a system: to use of components of better quality/maintainability, to substitute the component with a redundant configuration, to modify the Fault-tree failure logic to represent the adopted system modification. The first two interventions do not require any modification of the involved fault trees.

CISA was already implemented in the past and applied with success to real systems. The proposed method, however, overcomes the main drawbacks of the previous implementation and introduces a more objective and coherent approach to implement the Importance and Sensitivity Analysis procedure. In particular an attempt to reduce the occurrence probability of each Top-event is conduced in a selective manner by considering the estimated risk of the associated scenarios. To achieve this objective, different probability goals are selected for the different Top-events, depending on their specific contribution to risk.

Another innovative aspect of the proposed approach is that CISA is not solely used to address the most critical components in terms of their contribution to risk, but it also focuses on those less critical components, which may be uselessly reliable. In this way the application of the method is extended to the consideration of functions whose failure probability can be increased without compromising the requirements at Top-event level. The identification of these components may provide a contribution to costs reduction during the design phase, by still satisfying the probabilistic goals at the same time.

A dedicated software package (CISA) has been developed by the JRC to implement the proposed approach. Amongst the several features, this module allows to conduct a probabilistic analysis of multiple Fault-trees after any modification of the relevant basic events/components, the calculation of components' global importance measures, and check of probabilistic goal achievement. The system can be improved by substituting the critical component with a redundant configuration selected from a set of configurations. This module will be tested, and possibly improved, on real system cases.

The methodology described in this report represents an intermediate result of the project. Indeed, the following aspects are going to be developed:

- the extension to deal with catastrophic top events, for which the parameter of interest is the accident occurrence probability, expressed in terms of the expected number of failures;
- the determination of the top-event uncertainty, which is fundamental when dealing with the achievement of goals;

REFERENCES

1 S. Contini, S. Sheer, M. Wilikens, "Sensitivity Analysis for System Design Improvement", Proceedings of DSN 2000, New York

2 S. Contini, G. Cojazzi, G. Renda, G. De Cola, " La metodologia ASTRA per l'analisi di affidabilita' di sistemi complessi", VGR 2004, Valutazione e Gestione del Rischio negli Insediamenti Civili ed Industriali, Pisa, 2004.

3 A. Baietto, "Il ruolo dell'analisi di sensitivita' per l'integrazione dei requisiti di affidabilita' e sicurezza nella progettazione di sistemi di controllo per applicazioni energetiche" Tesi di laurea, Politecnico di Torino, 1997.

4 S. Kaplan, B.J. Garrick, "On the quantitative definition of risk", Risk Analysis, Volume 1, Issue 1, Page 11-27, Mar 1981.

5 M. Rausand, A. Hoyland, "System Reliability Theory. Models, Statistical Methods and Applications", 2nd Edition, Wiley Series in Probability and Statistics, 2004, ISBN 0-471-47133-X.

6 E. Borgonovo, G.E. Apostolakis, "A New Importance Measure for Risk-Informed Decision Making", Reliability Engineering & System Safety, 72 (2001), p. 193-212.

7 A. Rauzy, "A brief introduction to Binary Decision Diagrams" RAIRO-APII-JESA, European Journal of Automation, Vol. 30-n.8/1996.

8 A.E. Green, A.J. Bourne, Reliability Technology, Wiley-Interscience, 1977, ISBN 0-471-32480-9.

9 H. Kumamoto, E.J. Henley, Probabilistic Risk Assessment and Management for Engineers And Scientists, 2nd Edition, IEEE Press, 1996, ISBN 0-7803-1004-7

10 K.B. Misra, Reliability Analysis and Prediction, Elsevier, 1992, ISBN 0-444-89606-6

APPENDIX: LIBRARY OF REDUNDANT CONFIGURATIONS

This appendix describes the equations that are applied to determine both the unavailability Q(t) and the failure intensity ω(t) of some basic redundant configurations made up by equal repairable/not repairable/tested components. Other configurations can be added in the future according to the users' need. In CISA, a basic event (BE) is characterized by exponential distributions for the time to failure and the time to repair. Each BE selected for design improvement can be substituted with a redundant subsystem in a way that the analyst does not need to modify the Fault-tree structure. More precisely the unavailability and the failure rate of a BE, q(t) and λ, which are needed to determine the Top-event unavailability $Q_S(t)$ and Expected Number of Failure $W_S(t)$, are substituted with $Q_C(t)$ and $\omega_C(t)$ of the selected redundant configuration.

To define the redundant configuration library, the following data have to be specified.

Component parameters:
λ failure rate;
τ repair time, equal to $\tau = 1/\mu$;
q unavailability on demand;
θ test interval;
θ_0 time to first test;
γ test duration.

Redundant configuration parameters:
N = number of components;
R = number of repairmen ($1 \leq R \leq N$);

Allowable types of components:

Not repairable component:	$q = 1 - \exp(-\lambda t)$;
Repairable component (revealed failure)	$q = \lambda / (\lambda + \mu) [1 - \exp(-\lambda + \mu) t]$;
Inspected component	$q = 0.5 \lambda \theta + \lambda \tau + \gamma / \theta$.

Types of redundant configurations:
Parallel
Stand-by with perfect switching
cold $\lambda^* = 0$ (default)
warm $\lambda^* << \lambda$
K/N of active components
K/N of tested components subject to different testing policy: sequential; staggered.

Working Hypotheses:
equal components;
λ, μ constants;

Results at mission time T.
Redundant configurations with repairable components:
- Steady-state Unavailability;
- Failure frequency (unconditional) ω_C.

Redundant configurations with non repairable components:
- Unreliability;
- Mean Time To Failure (MTTF).

A.1 Parallel configuration of repairable components (steady state behavior)

Let N be the number of repairable components and R be the number of repairmen. The Repair policy is FIFO (First-In –First-Out). Components are supposed to be equal. The system failure occurs when all N components are failed.

The equations for determining the unavailability and unconditional failure frequency for different types of configurations make use of a Markov diagram. The generic state of the Markov diagram contains information about:

S = state number;
W = number of working components;
F = number of failed components.

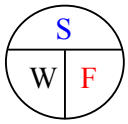


Figure A.1 shows the Markov transition diagram for the parallel configuration of interest. The transitions from states are associated with the failure / repair rates.

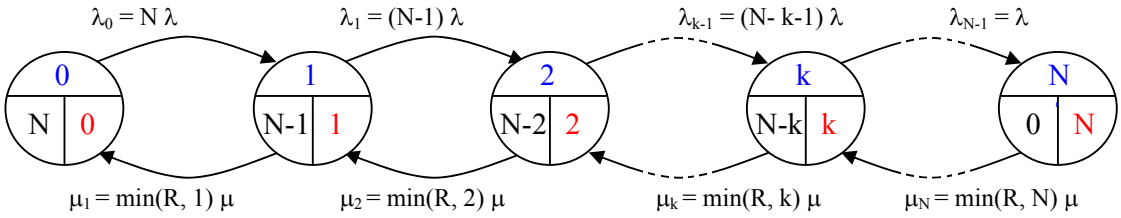


Figure A.1 Markov transition diagram for the determination of the steady state unavailability of parallel redundant configurations.

For a redundant configuration with N equal components, the number of states is N+1, in which N is the number of working states and the last one is the failed state.

The transitions between two generic states can be expressed as follows:

$\lambda_k = (N-K)\,\lambda$ for $0 \le K \le N-1$ (A.1)

$\mu_k = \min(R, K)\,\mu$ for $1 \le K \le N$ (A.2)

where the subscript indicates the state identification number from which the transition leaves.

For each state a differential equation is written according to the following procedure:

$\frac{dP_K}{dt}$ = (total inflow to state K) – (total outflow from state K), i.e.:

$$\frac{dP_K}{dt} = \sum_{j \neq K} \nu(j,K)\, P_j - \sum_{j \neq K} \nu(K,j)\, P_K$$

where $\nu(j,K)$ is the transition rate to state K from state j and $\nu(K,j)$ is the transition rate from state j to state K; P_j , P_K are respectively the probabilities of states j, K.

With reference to the Markov graph in Figure A.1 the application of the above rule to each state gives the following system of (N+1) differential equations.

$$\begin{cases} \dfrac{dP_0}{dt} = -\lambda_0\ P_0 + \mu_1\ P_1 \\ ..... \\ \dfrac{dP_K}{dt} = \lambda_{K-1}\ P_{K-1} - (\lambda_K + \mu_K)\ P_K + \mu_{K+1}\ P_{K+1} \qquad \text{for k=1,….,N-1} \\ ..... \\ \dfrac{dP_N}{dt} = \lambda_{N-1}\ P_{N-1} - \mu_N\ P_N \end{cases} \tag{A.3}$$

The initial condition is: $P_0=1$; $P_j=0$ for j=1,..,N, i.e. at t = 0 all components are working

Moreover $\sum_{K=0}^{N} P_K = 1$

For CISA purposes, it is sufficient to consider the steady-state unavailability of redundant configurations made up by equal components. In this case all derivatives are zero: the system (A.3) becomes a system of algebraic equations.

$$\begin{cases} -\lambda_0\ P_0 + \mu_1\ P_1 = 0 \\ ..... \\ \lambda_{K-1}\ P_{K-1} - (\lambda_K + \mu_K)\ P_K + \mu_{K+1}\ P_{K+1} = 0 \qquad \text{for k=1,….,N-1} \\ ..... \\ \lambda_{N-1}\ P_{N-1} - \mu_N\ P_N = 0 \end{cases} \tag{A.4}$$

The above system can be re-written as follows:

$$\begin{cases} \lambda_0\ P_0 - \mu_1\ P_1 = 0 \\ ..... \\ (\lambda_{K-1}\ P_{K-1} - \mu_K P_K) - (\lambda_K\ P_K - \mu_{K+1}\ P_{K+1}) = 0 \\ ..... \\ \lambda_{N-1}\ P_{N-1} - \mu_N\ P_N = 0 \end{cases}$$

In which the generic term $\lambda_{K-1}\ P_{K-1} - \mu_K\ P_K = 0$ appears. Since all $\mu_K \neq 0$, then $P_K = \dfrac{\lambda_{K-1}}{\mu_K} P_{K-1}$ for k=1,….,N.

$$\begin{cases} P_1 = \dfrac{\lambda_0}{\mu_1}\ P_0 \\ P_2 = \dfrac{\lambda_1}{\mu_2}\ P_1 \\ ..... \\ P_N = \dfrac{\lambda_{N-1}}{\mu_N}\ P_{N-1} \end{cases}$$

Therefore: $P_K = \dfrac{\lambda_0\ \lambda_1\ \lambda_2 .... \lambda_{K-1}}{\mu_1\ \mu_2\ \mu_3 .... \mu_K} P_0$ for k=1,….,N. (A.5)

Since $\sum_{K=0}^{N} P_K = 1$ it is straightforward to obtain:

$$P_0 + \frac{\lambda_0}{\mu_1} P_0 + \frac{\lambda_0\ \lambda_1}{\mu_1\ \mu_2} P_0 + \frac{\lambda_0\ \lambda_1\ \lambda_2}{\mu_1\ \mu_2\ \mu_3} P_0 + \frac{\lambda_0\ \lambda_1\ \lambda_2 \ldots.\ \lambda_{K-1}}{\mu_1\ \mu_2\ \mu_3 \ldots.\ \mu_K} P_0 + \ldots. + \frac{\lambda_0\ \lambda_1\ \lambda_2 \ldots.\ \lambda_{N-1}}{\mu_1\ \mu_2\ \mu_3 \ldots.\ \mu_N} P_0 = 1$$

Setting $S_x = \frac{\lambda_0\ \lambda_1\ \lambda_2 \ldots.\ \lambda_{x-1}}{\mu_1\ \mu_2\ \mu_3 \ldots.\ \mu_x}$ for x=1,….,N, then: $P_0 = \frac{1}{1 + \sum_{x=1}^{N} S_x}$

Finally: $P_K = \frac{S_K}{1 + \sum_{x=1}^{N} S_x}$

The steady state unavailability Q_C is the probability associated with the failed state N, i.e.:

$$Q_C = Q_N = \frac{S_N}{1 + \sum_{x=1}^{N} S_x} \qquad \text{(A.6)}$$

with

$$S_x = \frac{\prod_{j=0}^{x-1} \lambda_j}{\prod_{j=1}^{x} \mu_j} \qquad \text{(A.7)}$$

The frequency of visiting the failed state (unconditional failure frequency ω_S) is given by the probability that the system is in a critical state (the state N-1) times the probability of transition into the failed state (N). A state is said to be critical when only one component is working, whose failure leads to system failure.

Hence:

$$\omega_C = Q_{N-1}\, \lambda_{N-1} \qquad \text{(A.8)}$$

where

$$Q_{N-1} = \frac{S_{N-1}}{1 + \sum_{x=1}^{N} S_x} \qquad \text{(A.9)}$$

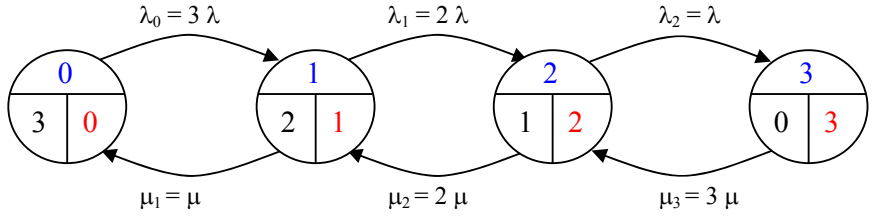
Example 1

As an example of application of the above equations, let's consider the case of three equal components (N=3) connected in parallel with three repairmen (R=3). This is the simple case of independent components for which it is well known that Q_C is given by the product of the components' unavailability. The Markov diagram can be derived from Figure A.1 where the transition rates assume the following values:

$\lambda_0 = 3\,\lambda$ $\quad\quad$ $\mu_1 = \mu$

$\lambda_1 = 2\,\lambda$ $\quad\quad$ $\mu_2 = 2\,\mu$

$\lambda_2 = \lambda$ $\quad\quad$ $\mu_3 = 3\,\mu$



Applying equations (A.7) to determine the terms for the application of equation (A.6) we get:

$$S_1 = \frac{\lambda_0}{\mu_1} = \frac{3\,\lambda}{\mu}$$

$$S_2 = \frac{\lambda_0 \cdot \lambda_1}{\mu_1 \cdot \mu_2} = \frac{3\,\lambda \cdot 2\,\lambda}{\mu \cdot 2\,\mu} = \frac{3\,\lambda^2}{\mu^2}$$

$$S_3 = \frac{\lambda_0 \cdot \lambda_1 \cdot \lambda_2}{\mu_1 \cdot \mu_2 \cdot \mu_3} = \frac{3\,\lambda \cdot 2\,\lambda \cdot \lambda}{\mu \cdot 2\,\mu \cdot 3\,\mu} = \frac{\lambda^3}{\mu^3}$$

$$Q_C = \frac{S_3}{1 + \sum_{x=1}^{3} S_x} = \frac{S_3}{1 + S_1 + S_2 + S_3} = \frac{\lambda^3}{(\lambda + \mu)^3} \quad \text{as expected.}$$

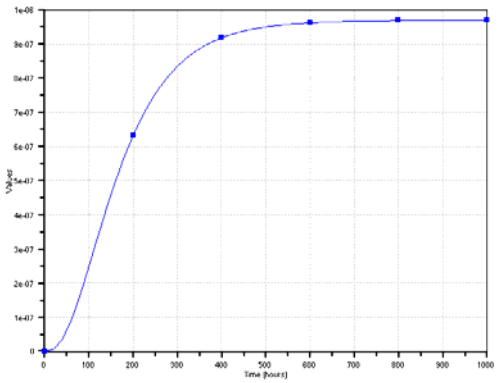
The product of the unavailability of critical states and the total failure rate of the exit branches gives the unconditional failure frequency.

$\omega_S = Q_2\,\lambda_2$ $\quad\quad$ where $Q_2 = \dfrac{S_2}{1 + \sum_{x=1}^{3} S_x} = \dfrac{3\,\lambda^2\,\mu}{(\lambda + \mu)^3}$

It follows that:

$$\omega_C = \frac{3\,\lambda^3\,\mu}{(\lambda + \mu)^3}$$

Let λ = 1e-4 and μ = 1e-2. From the plot of the unavailability shown below for this case it can be seen that the steady state value Q_C= 9.7e-7 is reached at about 600 h

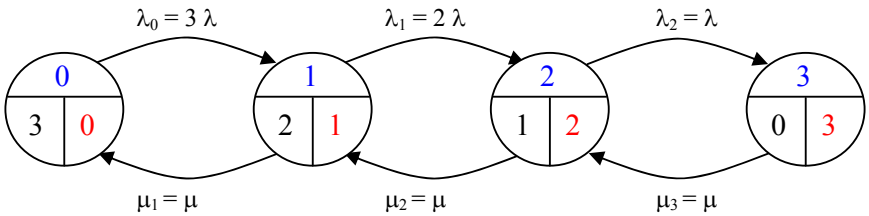


Plot of the unavailability vs. time for the first 1000h

Example 2

This second example still deals with the parallel of three components but considering a single repairman, i.e. N = 3, R = 1.

From the state diagram in Figure A1 the following graph s obtained by applying rules (A.1) and (A.2):



Applying equations (A.7) to determine the terms for the application of equation (A.6) we get:

$$S_1 = \frac{\lambda_0}{\mu_1} = \frac{3\,\lambda}{\mu} \qquad S_2 = \frac{\lambda_0 \cdot \lambda_1}{\mu_1 \cdot \mu_2} = \frac{3\,\lambda\,2\,\lambda}{\mu^2} = \frac{6\,\lambda^2}{\mu^2} \qquad S_3 = \frac{3\,\lambda\,2\,\lambda\,\lambda}{\mu^2} = \frac{6\,\lambda^3}{\mu^3}$$

From equation (A.6):

$$Q_C = \frac{S_3}{1+S_1+S_2+S_3} = \frac{6\,\lambda^3}{\mu^3+3\,\lambda\,\mu^2+6\,\lambda^2\mu+6\,\lambda^3}$$

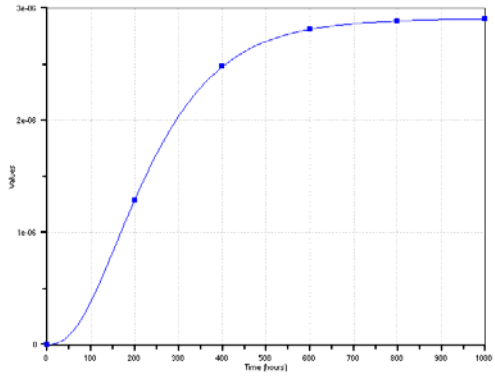
Concerning the calculation of the failure frequency:

$$Q_2 = \frac{S_2}{1+\sum_{x=1}^{3} S_x} = \frac{6\,\lambda^2\,\mu}{\mu^3+3\mu^2\lambda+6\lambda^2\mu+6\lambda^2}$$

Hence:

$$\omega_C = Q_2 \cdot \lambda_2 = \frac{6\,\lambda^3\mu}{\mu^3+3\,\lambda\,\mu^2+6\,\lambda^2\mu+6\,\lambda^3}$$

As before let λ = 1e-4 and μ = 1e-2. From the plot of the unavailability for this case it can be seen that the steady state value Q_C= 2.9e-6 is reached at about 800 h. As expected the unavailability with one repairman is greater than the unavailability with three repairmen.



Plot of the unavailability vs. time for the first 1000h

A.2 M–out-of-N configuration of active repairable components

Let N be the number of repairable components whose failure logic is represented as a series of M elements (M<N) in parallel; the system is failed if at least M out of N components are failed. Components are equal. R is the number of repairmen. The Repair policy is still of the type FIFO (First-In –First-Out).

The equations for determining the unavailability and unconditional failure frequency for different types of configurations make use of the same Markov diagrams represented in Figure A.1 for the parallel configuration of equal components. In this case, however, the number of working states is not N but M; consequently the number of failed states is not 1 but N-M+1. Therefore the steady-state unavailability is given by:

$$Q_C = \sum_{K=N-M+1}^{N} Q_K \qquad \text{(A.10)}$$

where Q_K can be determined applying equation (A.6) and (A.7).

$$Q_K = \frac{S_K}{1+\sum_{x=1}^{N} S_x}$$

$$S_x = \frac{\prod_{j=0}^{x-1`} \lambda_j}{\prod_{j=1}^{x} \mu_j}$$

Concerning the failure frequency:

$$\omega_C = Q_{N-M}\ \lambda_{N-M} \qquad \text{(A.11)}$$

where

$$Q_{N-M} = \frac{S_{N-M}}{1+\sum_{x=1}^{N} S_x} \qquad \text{and} \qquad S_{N-M} = \frac{\prod_{j=0}^{N-M-1`} \lambda_j}{\prod_{j=1}^{N-M} \mu_j}$$

In conclusion, this configuration is similar to the parallel configuration; the difference relates on the number of failed states (1 for parallel, N-M+1 for M out of N)

Example 3

Let's consider the 2/3 configuration with three repairmen, i.e. with independent components, for which the steady state unavailability expression is known, given by:

$$Q_C = 3\,q^2 - 2\,q^3 = \frac{3\,\lambda^2\,\mu + \lambda^3}{(\lambda+\mu)^3} \qquad \text{(A.12)}$$

In this example:

N = 3 M =2 R = 3

According to (A.1) and (A.2) the failure and repair transition rates are given by:

$\lambda_0 = 3\lambda$ $\mu_1 = \mu$

$\lambda_1 = 2\lambda$ $\mu_2 = 2\mu$

$\lambda_2 = \lambda$ $\mu_3 = 3\mu$

The S_x terms, for x=1,...,N, are given by:

$$S_1 = \frac{\lambda_0}{\mu_1} = \frac{3\lambda}{\mu}$$

$$S_2 = \frac{\lambda_0\,\lambda_1}{\mu_1\,\mu_2} = \frac{3\lambda^2}{\mu^2}$$

$$S_3 = \frac{\lambda_0\,\lambda_1\,\lambda_2}{\mu_1\,\mu_2\,\mu_3} = \frac{\lambda^3}{\mu^3}$$

Hence:

$$S = 1 + S_1 + S_2 + S_3 = 1 + \frac{3\lambda}{\mu} + \frac{3\lambda^2}{\mu^2} + \frac{\lambda^3}{\mu^3} = \frac{(\lambda+\mu)^3}{\mu^3}$$

Now $Q_K = \frac{S_K}{S}$ for k = 2, 3 are calculated, giving:

$$Q_2 = \frac{3\lambda^2}{S\,\mu^2} \qquad Q_3 = \frac{\lambda^3}{S\,\mu^3}$$

Finally, using equation (A.8):

$$Q_C = \sum_{K=N-M+1}^{N} Q_K = \sum_{K=2}^{3} Q_K = \frac{3\,\lambda^2\,\mu + \lambda^3}{(\lambda+\mu)^3}$$

which is equal to expression (A.12)

Concerning the unconditional failure frequency:

$$Q_{N-M} = \frac{S_{N-M}}{1 + \sum_{x=1}^{N} S_x} \text{ gives } Q_1 = \frac{S_1}{S} = \frac{3\lambda}{S\,\mu} = \frac{3\lambda\,\mu^2}{(\lambda+\mu)^3}$$

$$\omega_C = Q_{N-M}\,\lambda_{N-M} \text{ gives } \omega_C = \frac{6\lambda^2\,\mu^2}{(\lambda+\mu)^3}$$

Example 4

Let's consider again the 2/3 configuration but with one repairman only, i.e. with dependent components. In this case:

N = 3, M =2, R = 1

According to (A.1) and (A.2) the failure and repair transition rates are given by:

$\lambda_0 = 3\lambda$ $\mu_1 = \mu$

$\lambda_1 = 2\lambda$ $\mu_2 = \mu$

$\lambda_2 = \lambda$ $\mu_3 = \mu$

The S_x terms, for x=1,...,N, are given by:

$$S_1 = \frac{\lambda_0}{\mu_1} = \frac{3\lambda}{\mu}$$

$$S_2 = \frac{\lambda_0\ \lambda_1}{\mu_1\ \mu_2} = \frac{6\lambda^2}{\mu^2}$$

$$S_3 = \frac{\lambda_0\ \lambda_1\ \lambda_2}{\mu_1\ \mu_2\ \mu_3} = \frac{6\lambda^3}{\mu^3}$$

Hence:

$$S = 1 + S_1 + S_2 + S_3 = 1 + \frac{3\lambda}{\mu} + \frac{6\lambda^2}{\mu^2} + \frac{6\lambda^3}{\mu^3} = \frac{\mu^3 + 3\ \lambda\ \mu^2 + 6\ \lambda^2\ \mu + 6\lambda^3}{\mu^3}$$

Now $Q_K = \frac{S_K}{S}$ for k = 2, 3 are calculated, giving:

$$Q_2 = \frac{6\lambda^2}{S\ \mu^2} \qquad Q_3 = \frac{6\lambda^3}{S\ \mu^3}$$

Finally, using equation (A.10):

$$Q_C = \sum_{K=N-M+1}^{N} Q_K = \sum_{K=2}^{3} Q_K = \frac{6\ \lambda^2\ \mu + 6\lambda^3}{\mu^3 + 3\ \lambda\ \mu^2 + 6\ \lambda^2\ \mu + 6\lambda^3}$$

Concerning the unconditional failure frequency:

$$Q_{N-M} = \frac{S_{N-M}}{1 + \sum_{x=1}^{N} S_x} \text{ gives } Q_1 = \frac{S_1}{S} = \frac{3\lambda}{S\ \mu} = \frac{3\lambda\ \mu^2}{\mu^3 + 3\ \lambda\ \mu^2 + 6\ \lambda^2\ \mu + 6\lambda^3}$$

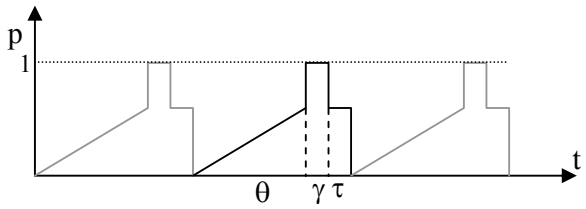
$$\omega_C = Q_{N-M}\ \lambda_{N-M}$$

gives $\omega_C = \frac{6\ \lambda^2\ \mu^2}{\mu^3 + 3\ \lambda\ \mu^2 + 6\ \lambda^2\ \mu + 6\lambda^3}$

A.3 M-out-of-N tested/inspected components (M out of N: B logic)

This configuration is used for modelling protective functions for which the unavailability on demand is the parameter of interest. Components are in stand-by position ready to intervene in case of request to stop the escalation of a hazardous plant condition. If the failure of these components is not revealed then the components' integrity can be verified only through periodical tests. After the test, if the component is found failed it is immediately repaired.
The mean unavailability for this type of components is given by:

$$q = \frac{1}{2}\lambda\,\theta + \frac{\gamma}{\theta} + \lambda\,\tau$$



where the first term accounts for the mean unavailability between two successive tests under the condition that $\lambda\,\theta < 0.1$; the second term is the contribution due to test (the test makes the component unavailable); the last term is the contribution due to repair if the component is found failed, which is given by the unavailability due to repair (τ / θ) times the probability that the component is failed at θ ($\lambda\,\theta$). In the above equation $\tau+\gamma << \theta$; hence in what follows $\theta + \tau + \gamma \cong \theta$.

A demand for the component action may occur during the test. If the component can respond, i.e. if there is the "override capability" then $\gamma = 0$. In the above equation the probability that the test might fail the component (human error) is considered negligible.

Any M/N failure logic is modelled as a series of parallel configurations, e.g. a 2/3 is represented as a series of 3 subsystems each one made up by 2 items in parallel. More generally, for an M/N configuration, the number of parallels of M components connected in series is given by:

$$\binom{N}{M} = \frac{N!}{M!\,(N-M)!}$$

The unavailability of the M/N configuration made up by equal components is given by:

$$Q_C = \binom{N}{M}[Q_1 + Q_2 + Q_3] \qquad \text{(A.13)}$$

where Q_1, Q_2, Q_3 are respectively the mean unavailability contributions due to the three time periods in which failures are undetected (duration θ), components are under test (duration γ), and under repair (duration τ).

Equation (A.13) has been implemented in CISA for two testing policies:

- Sequential;
- Staggered.

The *sequential testing policy* is such that components are tested one after the other in such a way that only one component at a time is put off-line for testing.

The *staggered testing policy* is such that components are tested regularly in an overlapping sequence; given the parallel of *n* components, each component is tested every θ hours, but the time between two successive tests (involving a different components) is θ/n hours. For instance, if n=3 and θ = 3000h,

the first component is tested at 1000h, the second at 2000h, the third at 3000h, the first again at 4000h, and so on.

The equations for determining the three contributors to the mean unavailability of a *generic parallel of n equal components* are briefly described below.

Contribution to the unavailability because of failure between tests

Sequential testing
Between tests components' failures are not revealed, i.e. they are not repairable. Therefore the mean unavailability of *n* components in parallel, under the hypothesis that $\lambda\ \theta < 0.1$ is given by:

$$Q_1 = \frac{1}{\theta}\int_0^{\theta} \lambda^n\ t^n dt = \frac{1}{n+1}\lambda^n\ \theta^n \qquad \text{(A.14)}$$

Staggered testing
The contribution in case of staggered testing is given by [8]:

$$Q_1 = \frac{n!\,(n+3)}{4\,n^n\,(n+1)}\lambda^n\ \theta^n \qquad \text{(A.15)}$$

Contribution to the unavailability because of testing

Sequential testing
When the first component is tested, its contribution to the unavailability is γ/θ, whereas the probability that the other components (the parallel of n-1 components) are failed at θ is $\lambda^{n-1}\ \theta^{n-1}$; when the second component is tested its contribution to the unavailability is $\gamma\ /\ \theta$ but now one component (the first tested) has unavailability $\lambda\ \gamma$ and the unavailability of the remaining components (still to be tested) is $\lambda^{n-2}\ \theta^{n-2}$, and so on. Therefore for a generic parallel of n elements the total contribution is given by:

$$Q_2 = \frac{\gamma}{\theta}[\lambda^{n\ 1}\theta^{n\ 1} + \lambda^{n\ 2}\theta^{n\ 2}\ \lambda\ \gamma + \lambda^{n\ 3}\theta^{n\ 3}\ \lambda^2\ \gamma^2 + ...] = \sum_{j=1}^{n} \lambda^{n-j}\ \theta^{n-j-1}\ \gamma^j$$

For a generic $j > 1$ the corresponding term is about θ times smaller than the previous term. Hence it is reasonable to retain the first term only, i.e.:

$$Q_2 = \lambda^{n-1}\ \theta^{n-2}\ \gamma \qquad \text{(A.16)}$$

Staggered testing
When the first component is tested its contribution to the unavailability is γ/θ, whereas the probability that all other (n-1) components are failed at the initial of the test period γ is given by:

$$\lambda\frac{\theta}{n}\cdot\lambda\frac{2\theta}{n}\cdot\lambda\frac{3\theta}{n}\cdot\ldots\cdot\lambda\frac{(n-1)\theta}{n} = \frac{(n-1)!}{n^{n-1}}\lambda^{n-1}\ \theta^{n-1}$$

Therefore: $Q(1\ on\ test) = \frac{\gamma}{\theta}\frac{(n-1)!}{n^{n-1}}\lambda^{n-1}\ \theta^{n-1} = \frac{(n-1)!}{n^{n-1}}\lambda^{n-1}\ \theta^{n-2}\ \gamma$

Other smaller contributions can be added accounting for the failure of one or more components during the test period γ. Since γ << θ these contributions are very small compared with the above, which means that they can reasonably be neglected.
Hence it is sufficient to multiply the unavailability due to one component under test to the number of components to obtain the test-unavailability contribution Q_2, i.e.:

$$Q_2 = \frac{(n-1)!}{n^{n-2}} \lambda^{n-1}\ \theta^{n-2}\ \gamma \qquad \text{(A.17)}$$

Contribution to the unavailability because of repair

Sequential testing
When the first component is found failed after test it has to be repaired. The contribution of repair to the unavailability is λ τ, whereas the probability that the other n-1 components are failed at the beginning of the repair period is $\lambda^{n-1}\ \theta^{n-1}$.
When the second component is tested its contribution to the unavailability is λ τ, but now the first tested component has mean unavailability λ τ and the unavailability of the remaining components (still to be tested) is $\lambda^{n-2}\ \theta^{n-2}$, and so on. Hence:

$$Q_3 = \lambda\ \tau\ [\lambda^{n\ 1}\theta^{n\ 1} + \lambda^{n\ 2}\theta^{n\ 2}\ \lambda\ \tau + \lambda^{n\ 3}\theta^{n\ 3}\ \lambda^2\ \tau^2 + ...] = \sum_{j=1}^{n} \lambda^n\ \theta^{n-j}\ \tau^j$$

As j increases, the corresponding term is about θ times smaller than the previous term. As for (A.16) it is reasonable to retain the first term only, i.e.:

$$Q_3 = \lambda^n\ \theta^{n-1}\ \tau \qquad \text{(A.18)}$$

Staggered testing
When the first component is under repair, its contribution to the unavailability is λτ, whereas the probability that the other (n-1) components be failed at θ is given by:

$$\lambda\frac{\theta}{n} \cdot \lambda\frac{2\theta}{n} \cdot \lambda\frac{3\theta}{n} \cdot \ldots \cdot \lambda\frac{(n-1)\theta}{n} = \frac{(n-1)!}{n^{n-1}} \lambda^{n-1}\ \theta^{n-1}.$$

Other smaller contributions can be added accounting for the failure of one or more components during the repair period τ. Since τ << θ these contributions are very small compared with the above, which means that they can reasonably be neglected.
Hence it is sufficient to multiply the unavailability due to one component under repair to the number of components to obtain the repair-unavailability contribution Q_3, i.e.:

$$Q_3 = \frac{(n-1)!}{n^{n-2}} \lambda^n\ \theta^{n-1}\ \tau \qquad \text{(A.19)}$$

The above equations applied to parallel configurations up to order 5 are given in the following Table.

It is easy to see that from the mean unavailability point of view the staggered testing policy is better than the sequential testing policy.

M	Sequential	Staggered
2	$\frac{1}{3}\lambda^2\ \theta^2 + \lambda\ \gamma + \lambda^2\ \theta\ \tau$	$\frac{5}{24}\lambda^2\ \theta^2 + \lambda\ \gamma + \lambda^2\ \theta\ \tau$
3	$\frac{1}{4}\lambda^3\ \theta^3 + \lambda^2\ \theta\ \gamma + \lambda^3\ \theta^2\ \tau$	$\frac{1}{12}\lambda^3\ \theta^3 + \frac{2}{3}\lambda^2\ \theta\ \gamma + \frac{2}{3}\lambda^3\ \theta^2\ \tau$
4	$\frac{1}{5}\lambda^4\ \theta^4 + \lambda^3\ \theta^2\ \gamma + \lambda^4\ \theta^3\ \tau$	$\frac{21}{890}\lambda^4\ \theta^4 + \frac{3}{8}\lambda^3\ \theta^2\ \gamma + \frac{3}{8}\lambda^4\ \theta^3\ \tau$
5	$\frac{1}{6}\lambda^5\ \theta^5 + \lambda^4\ \theta^3\ \gamma + \lambda^5\ \theta^4\ \tau$	$\frac{8}{625}\lambda^5\ \theta^5 + \frac{24}{125}\lambda^4\ \theta^3\ \gamma + \frac{24}{125}\lambda^5\ \theta^4\ \tau$

Example 5

In this example the exact results, obtained using the time dependent probabilistic analysis of ASTRA 3.0, are compared with the approximated results given by the application of the equations above described. Reference is made to a 2/3 configuration of equal components. $\Phi = a\ b + a\ c + b\ c$ with mission time of 9,000h.

Each component is characterised by the following data:

- failure rate $\lambda = 1.e\text{-}4$;
- repair time $\tau = 1$ h;
- test interval $\theta = 300$ h;
- test time: negligible (presence of the override capability).

Sequential testing policy.

Components are tested one after the other. Only one component is put off line, tested and immediately put on-line before testing the next component. Suppose that each component is tested in a period less than 1 h. Under these hypotheses the data used are as follows:

x	λ h^{-1}	τ h	θ h	θo h
A	1.e-4	1	300	0.0
B	1.e-4	1	300	1
C	1.e-4	1	300	2

The plot of the system unavailability is shown in the following figure.

The mean value is equal to 8.55 x 10^{-4}, which follows the behaviour (for the first 1,800h) displayed in the figure. The maximum value of the unavailability is 2.55 x 10^{-3}.

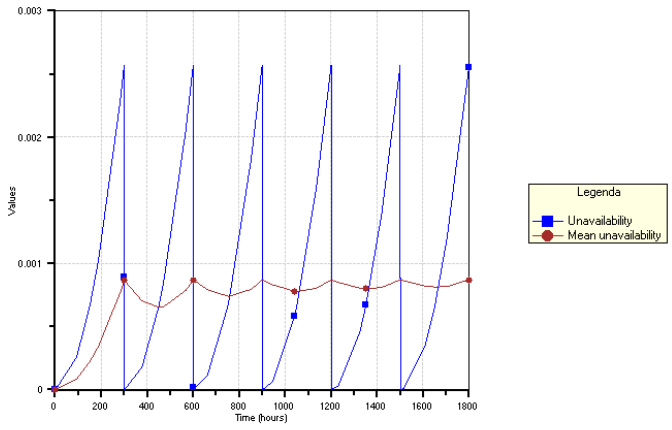


Figure A1. Unavailability of the 2/3 configuration (sequential testing policy).

Staggered testing policy.

Components are tested one after the other at regular intervals of time. If $\theta = 300$h is the test interval, then the first component is tested at t = 0 (first test at $\theta_0 = 0$), the second at $t = \theta / 3$ ($\theta_0 = 100$ h) and the third at $t = 2\theta /3$ (θo = 200 h). In the hypothesis that the time to test duration is negligible, the data used are as follows:

x	λ	τ	θ	θ_0
A	1.e-4	1	300	0.0
B	1.e-4	1	300	100
C	1.e-4	1	300	200

The plot of the system unavailability is shown in figure A2.
The mean value is equal to 5.558 x 10^{-4}, which follows the behaviour (for the first 1,800h) displayed in the figure. The maximum value of the unavailability is 1.06 x 10^{-3}.

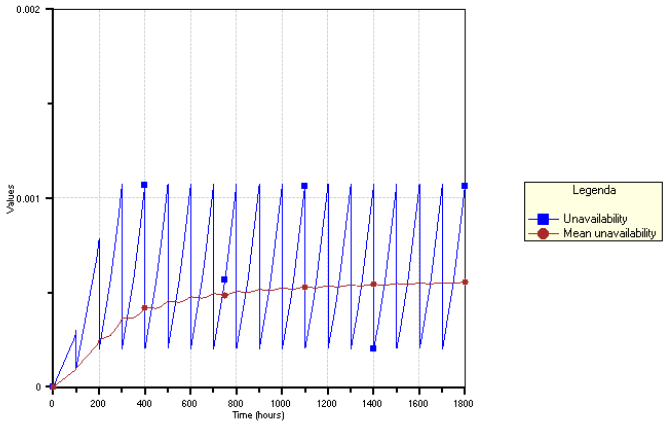


Figure A2. Unavailability of the 2/3 configuration (staggered testing policy).

Comparing the two policies it can be noticed, as expected, that the best one is the staggered testing.

The application of the approximated equations (A.3-A.19) gives the conservative results provided in the following table, in which the last column contains the relative error calculated with respect to the exact values determined by ASTRA 3.0.

Policy	Exact Mean Unavailability	Approximated Mean Unavailability	Relative error %
Sequential	8.55 x 10^{-4}	9.09 x 10^{-4}	6.3 %
Staggered	5.56 x 10^{-4}	5.7 x 10^{-4}	2.5 %

In order to get an idea about the degree of conservativeness of the approximated equations the previous example is re-considered in which the test interval is increased to 1000h, so that $\lambda\ \theta = 0.1$ (It is recommended not to exceed the value 0.1).

Results obtained from running ASTRA 3.0.

Policy	Exact Mean Unavailability	Approximated Mean Unavailability	Relative error %
Sequential	8.85 x 10^{-3}	1.0 x 10^{-2}	12.9 %
Staggered	5.89 x 10^{-3}	6.28 x 10^{-3}	6.6 %

A.4 Stand-by with repairable components and perfect switching

The following hypotheses are considered:

- N repairable and identical components;
- The redundant configuration has 1 on-line components and N-1 stand-by components;
- At most R components (R≥1) can be repaired at a time (R = number of repairmen);
- Maintenance policy: FIFO;
- Failure rate of the on-line components: λ;
- Failure rate of the components in stand-by: λ^*;
  - $\lambda^* = 0$ cold stand-by;
  - $\lambda^* = \lambda_0 << \lambda$ warm stand-by;
  - $\lambda^* = \lambda$ hot stand-by;
- Perfect switching;
- Components can fail only when in operation (Probability to start =1)

The system fails when N component fail. The reliability block diagram is as follows:

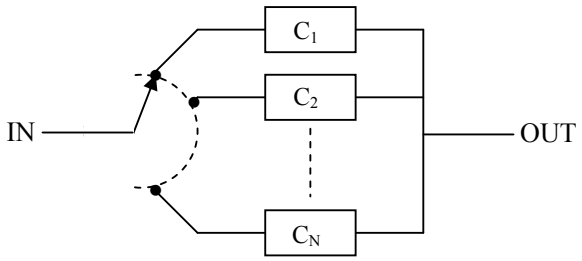
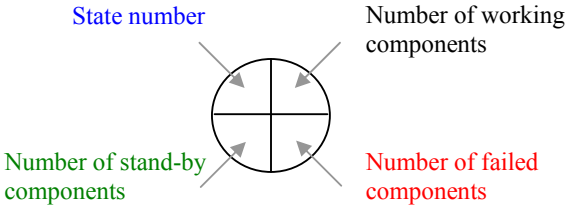


Figure A.2 RBD of a stand-by redundant configuration with 1 component on line and N-1 in stand-by

Each state of the state transition diagram contains the following information:



The state transition diagram is represented in Figure A.2.

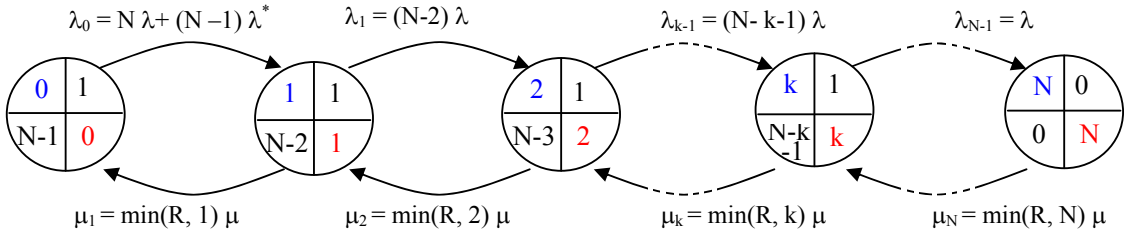


Figure A.3 Markov transition diagram for the determination of the steady state unavailability of stand-by redundant configurations with repairable components

Indicating with K the state number, the transition rates are given by:

$\lambda_K = \lambda + (N - K - 1)\,\lambda^*$ for $0 \le K \le N - 1$ (A.20)

$\mu_K = \min(R, K)\,\mu$ for $1 \le K \le N$

The stand-by unavailability at the steady state conditions can be calculated as follows:

$$Q_C = \frac{S_N}{1 + \sum_{x=1}^{N} S_x}$$

$$S_x = \frac{\prod_{j=0}^{x-1} \lambda_j}{\prod_{j=1}^{x} \mu_j}$$

Concerning the failure frequency:

$$\omega_C = Q_{N-1}\,\lambda_{N-1}$$

where,

$$Q_{N-1} = \frac{S_{N-1}}{1 + \sum_{x=1}^{N} S_x} \qquad \text{and} \qquad S_{N-1} = \frac{\prod_{j=0}^{N-2} \lambda_j}{\prod_{j=1}^{N-1} \mu_j}$$

Example 6

Stand-by sub-system with N = 3, M = 1, R = 1, and with perfect switching.
This configuration fails if the on-line component fails and if both stand –by components fail.

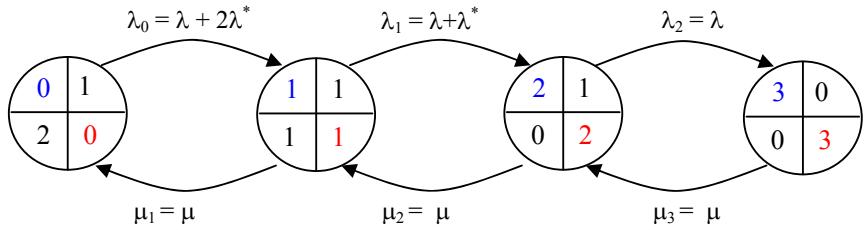
From (A.20):

$\lambda_0 = \lambda + 2\lambda^*$ $\quad\quad$ $\mu_1 = \mu$

$\lambda_1 = \lambda$ $\quad\quad$ $\mu_2 = \mu$

$\lambda_2 = \lambda$ $\quad\quad$ $\mu_3 = \mu$

The transition diagram is as follows:



$$Q_3 = \frac{S_3}{1 + \sum_{x=1}^{3} S_x} \quad \text{where:}$$

$$S_1 = \frac{\lambda_0}{\mu_1} = \frac{\lambda + 2\lambda^*}{\mu}$$

$$S_2 = \frac{\lambda_0\ \lambda_1}{\mu_1\ \mu} = \frac{\lambda^2 + 3\ \lambda\lambda^* + 2\lambda^{*2}}{\mu^2}$$

$$S_3 = \frac{\lambda_0\ \lambda_1\ \lambda_2}{\mu_1\ \mu_2\ \mu_3} = \frac{\lambda^3 + 3\ \lambda^2\lambda^* + 2\lambda\lambda^{*2}}{\mu^3}$$

$$1 + S_1 + S_2 + S_3 = \frac{\mu^3 + \lambda\mu^2 + 2\lambda^*\mu^2 + \lambda^2\mu + 3\lambda\lambda^*\mu + 2\ \lambda^{*2}\mu + \lambda^3 + 3\ \lambda^2\lambda^* + 2\lambda\lambda^{*2}}{\mu^3}$$

The above equations allow determining the steady-state unavailability in case of warm stand-by.

In case of cold stand-by, $\lambda^* = 0$, we have:

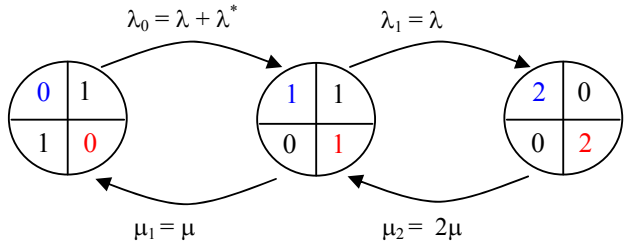
$$Q_3 = \frac{\lambda^3}{\mu^3 + \lambda\mu^2 + \lambda^2\mu + \lambda^3}$$

Concerning hot stand-by, $\lambda^* = \lambda$:

$$Q_3 = \frac{6\lambda^3}{\mu^3 + 6\lambda^2\mu + 3\lambda\mu^2 + 6\lambda^3}$$

Example 7

Stand-by sub-system with N = 2, M = 1, R = 2, and with perfect switching [9].
The transition diagram is as follows:



$$Q_2 = \frac{S_2}{1 + \sum_{x=1}^{2} S_x} \quad \text{where:}$$

$$S_1 = \frac{\lambda_0}{\mu_1} = \frac{\lambda + \lambda^*}{\mu}$$

$$S_2 = \frac{\lambda_0 \lambda_1}{\mu_1 \mu_2} = \frac{\lambda^2 + \lambda\lambda^*}{2\mu^2}$$

$$1 + S_1 + S_2 = \frac{2\mu^2 + 2\lambda\mu + 2\lambda^*\mu + \lambda^2 + \lambda\lambda^*}{2\mu^2}$$

In case of worm stand-by, $\lambda^* << \lambda$, we have:

$$Q_2 = \frac{\lambda^2 + \lambda\lambda^*}{2\mu^2 + 2\lambda\mu + 2\lambda^*\mu + \lambda^2 + \lambda\lambda^*}$$

In case of cold stand-by, $\lambda^* = 0$, we have:

$$Q_2 = \frac{\lambda^2}{2\mu^2 + 2\lambda\mu + \lambda^2}$$

Concerning hot stand-by, $\lambda^* = \lambda$:

$Q_3 = \frac{2\lambda^2}{2\mu^2 + 4\lambda\mu + 2\lambda^2} = \frac{\lambda^2}{(\lambda + \mu)^2}$, as expected, since it is equivalent to the parallel configuration of independent components.

A.5 Parallel of not repairable components

If components are all not repairable their repair rates are zero. Hence, the Markov transition diagram can be derived from the one in Figure A.1 by setting $\mu = 0$, i.e.:

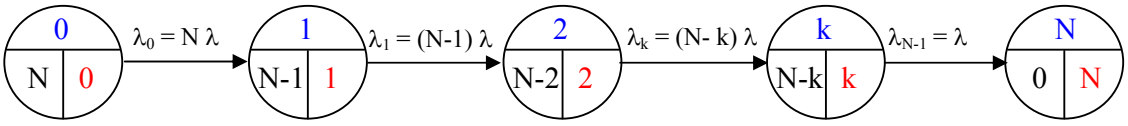


Figure A.4 Markov transition diagram for the determination of the unreliability of parallel redundancy

Also in this case for a redundant configuration with N equal components the number of states is N+1, in which N is the number of working states and the last one is the failed state.

Since components are equal, independent and with exponential failure distribution, then:

$Q_C(t) = [1 - q(t)]^N$ where $q(t) = e^{-\lambda t}$ is the component reliability at time t. (A.21)

It can be shown that in this case: $MTTF = \int_0^\infty R(t)\,dt = \frac{1}{\lambda}\sum_{j=1}^{N}\frac{1}{j}$ (A.22)

The following Table gives the expressions for the MTTF on N ranging from 1 to 5.

N	MTTF
1	$1/\lambda$
2	$3/2\lambda$
3	$11/6\lambda$
4	$25/12\lambda$
5	$137/60\lambda$

A.6 M/N Majority voting system with not repairable components

Given a system composed of N components, the system fails if at least M out of N components fail, indicated as M/N:B, where B stands for "Bad".
The Unreliability for M/N:B redundant configurations in the hypotheses of identical components can be calculated as:

$$Q_C(t) = 1 - \sum_{j=M}^{N}\binom{N}{M} e^{-j\lambda t}(1 - e^{-\lambda t})^{N-j} \quad \text{(A.23)}$$

It can also be shown that $MTTF = \int_0^\infty R(t)\,dt = \frac{1}{\lambda}\sum_{j=K}^{N}\frac{1}{j}$ (A.24)

The following Table gives examples of the MTTF for some M/N configurations of identical components.

M	**N**			
	2	**3**	**4**	**5**
1	1/2λ	1/3λ	1/4λ	1/5λ
2	---	5/6λ	7/12λ	9/20λ
3	---	---	13/12λ	47/60λ
4	---	---	---	77/60λ

A.7 Stand-by redundancy of not repairable components

Let N be the total number of components of the configuration, M=1 is the on–line component and N-1 the components in stand-by, ready to substitute the on-line component one after the other.
Suppose that the switching device is considered perfect. The reliability block diagram is the same as provided in Figure A.2

It can be shown that [10] the unreliability of a cold stand-by ($\lambda^* << \lambda$) is given by:

$$Q_C(t) = q\left[\sum_{j=0}^{N-1}\frac{(\lambda\, t)^j}{j!}\right] \qquad \text{(A.25)}$$

where $q = e^{-\lambda t}$ and t represents the mission time.

Moreover, it can easily be proved that: $MTTF = \frac{N}{\lambda}$ (A.26)

European Commission

EUR 23825 EN – Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Concurrent Importance and Sensitivity Analysis applied to multiple Fault-trees
Author(s): Sergio Contini, Luciano Fabbri and Vaidas Matuzas
Luxembourg: Office for Official Publications of the European Communities
2009 – 84 pp. – 21 x 29.7 cm
EUR – Scientific and Technical Research series – ISSN 1018-5593

Abstract
Complex industrial systems may present different potentially dangerous failure states (Top-Events). The analysis of system failure states via Fault-tree technique allows determining the failure frequency of potential accidents and the importance measures of components' failure modes. The combination of Importance and Sensitivity Analysis (ISA) constitutes a very powerful tool to improve the design of critical systems or to prove that the design satisfies safety requirements. The present reports describes a novel approach to implement Importance and Sensitivity analysis applied to Fault-trees, which consists of the concurrent analysis of all relevant system's Fault-trees to identify the weakest parts of the system which require further design improvement. This approach aims at overcoming the limitations of the current methods in application for ISA in which Top-events are sequentially analysed. In addition the proposed method extends the ISA application also to "over-reliable" system functions (if any) on which the reliability/maintainability characteristics of the involved components can be relaxed with consequent cost saving. The result of the analysis is a uniformly protected system satisfying the predefined design goals.

How to obtain EU publications

Our priced publications are available from EU Bookshop (http://bookshop.europa.eu), where you can place an order with the sales agent of your choice.

The Publications Office has a worldwide network of sales agents. You can obtain their contact details by sending a fax to (352) 29 29-42758.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.